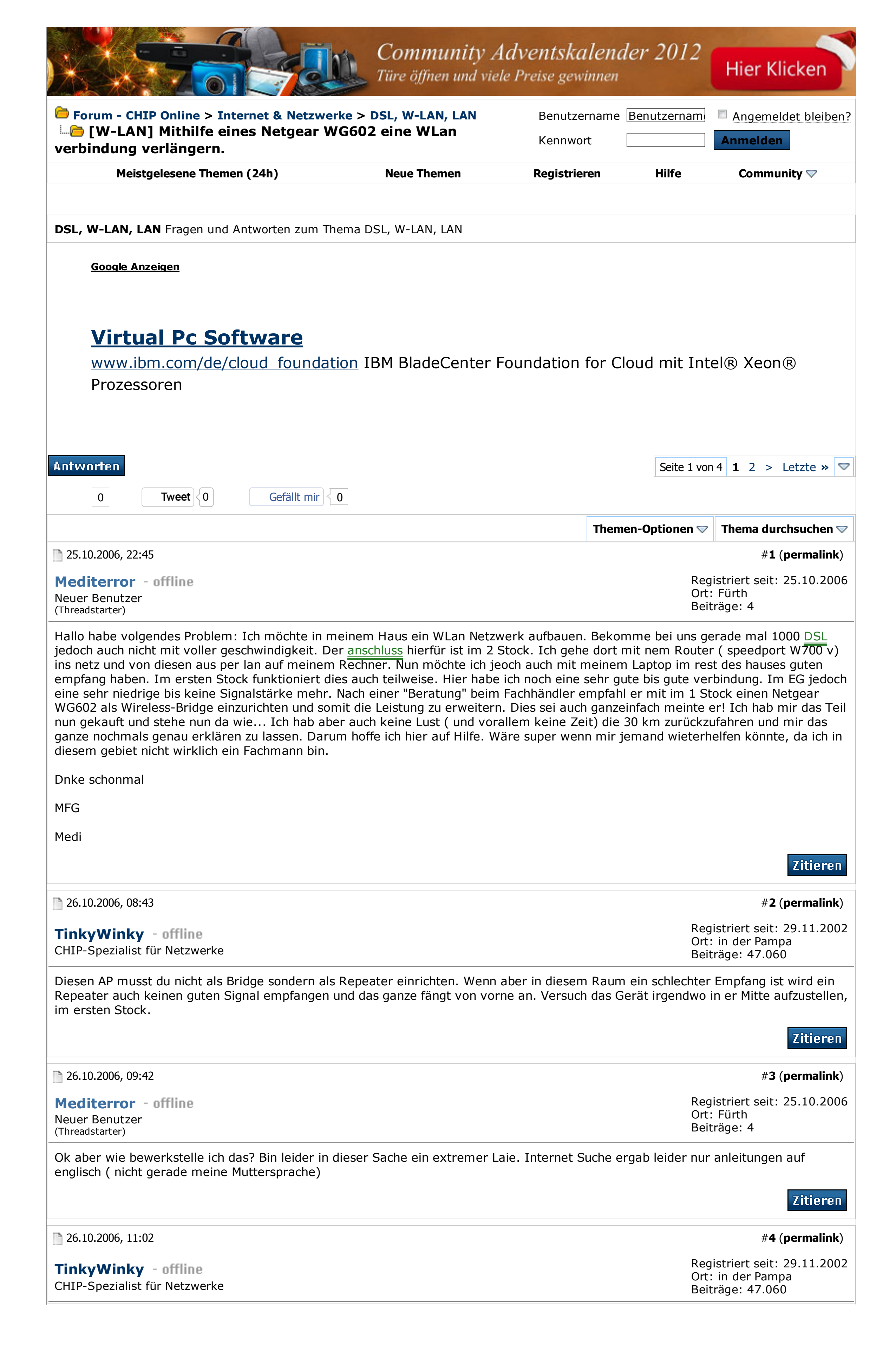


Forum - CHIP Online > Internet & Netzwerke > DSL, W-LAN, LAN
[W-LAN] Mithilfe eines Netgear WG602 eine WLan verbindung verlängern.

DSL, W-LAN, LAN Fragen und Antworten zum Thema DSL, W-LAN, LAN

25.10.2006, 22:45 #1 (permalink)

Mediterror - offline
Neuer Benutzer
(Threadstarter)
Registriert seit: 25.10.2006
Ort: Fürth
Beiträge: 4

Hallo habe volgendes Problem: Ich möchte in meinem Haus ein WLan Netzwerk aufbauen. Bekomme bei uns gerade mal 1000 DSL jedoch auch nicht mit voller geschwindigkeit. Der anschluss hierfür ist im 2 Stock. Ich gehe dort mit nem Router (speedport W700 v) ins netz und von diesen aus per lan auf meinem Rechner. Nun möchte ich jeoch auch mit meinem Laptop im rest des hauses guten empfang haben. Im ersten Stock funktioniert dies auch teilweise. Hier habe ich noch eine sehr gute bis gute verbindung. Im EG jedoch eine sehr niedrige bis keine Signalstärke mehr. Nach einer "Beratung" beim Fachhändler empfahl er mit im 1 Stock einen Netgear WG602 als Wireless-Bridge einzurichten und somit die Leistung zu erweitern. Dies sei auch ganzeinfach meinte er! Ich hab mir das Teil nun gekauft und stehe nun da wie... Ich hab aber auch keine Lust (und vorallem keine Zeit) die 30 km zurückzufahren und mir das ganze nochmals genau erklären zu lassen. Darum hoffe ich hier auf Hilfe. Wäre super wenn mir jemand wieterhelfen könnte, da ich in diesem gebiet nicht wirklich ein Fachmann bin.

Dnke schonmal

MFG

Medi

Zitieren

26.10.2006, 08:43 #2 (permalink)

TinkyWinky - offline
CHIP-Spezialist für Netzwerke
Registriert seit: 29.11.2002
Ort: in der Pampa
Beiträge: 47.060

Diesen AP musst du nicht als Bridge sondern als Repeater einrichten. Wenn aber in diesem Raum ein schlechter Empfang ist wird ein Repeater auch keinen guten Signal empfangen und das ganze fängt von vorne an. Versuch das Gerät irgendwo in er Mitte aufzustellen, im ersten Stock.

Zitieren

26.10.2006, 09:42 #3 (permalink)

Mediterror - offline
Neuer Benutzer
(Threadstarter)
Registriert seit: 25.10.2006
Ort: Fürth
Beiträge: 4

Ok aber wie bewerkstelle ich das? Bin leider in dieser Sache ein extremer Laie. Internet Suche ergab leider nur anleitungen auf englisch (nicht gerade meine Muttersprache)

Zitieren

26.10.2006, 11:02 #4 (permalink)

TinkyWinky - offline
CHIP-Spezialist für Netzwerke
Registriert seit: 29.11.2002
Ort: in der Pampa
Beiträge: 47.060

Rein theoretisch funktioniert es so:

1. Zuerst musst du deinen PC per Kabel mit dem AP verbinden. Nur diese LAN Verbindung sollte aktiv sein, alle anderen deaktivieren. Stelle den AP irgenwo in der Nähe des Routers hin. Schalte im Router die Verschlüsselung aus. Auch MAC Filter sollte ggf. deaktiviert werden. SSID soll sichtbar sein.

2. In den TCP/IP Eigenschaften der LAN Verbindung auf dem PC musst du eine IP manuell einragen. Welcher WG602 ist es? Wenn das ein WG 602v3 ist hat er die IP 192.168.1.227. Du musst also eine IP in diesem Bereich zuweisen. Nimm z.B. 192.168.1.222. Gateway und DNS ist hier egal, kann leer bleiben.

3. Jetzt öffnest du einen Browser und tippst 192.168.1.227 ein. Im Konfigmenu machst du folgendes:

a. Im Menu wireless Bridging stellst du "Repeater with Wireless Client Association" ein und trägst die MAC deines WLAN Routers ein. Die MAC Adresse findest du auf dem Typenschild beim Speedport. Mit "Apply" aktivierst du die Einstellung

b. In "Wireless Settings" trägst du die SSID ein die im Speedport eingetragen ist. Auch derselbe Kanal wie im Speedport muss eingetragen werden. Falls du die Werte nicht auswendig kennst notiere dir das bevor du mit der Einrichtung startest. Notiere dir auch die MAC Adresse des Netgears. Diese findest du ganz oben im Menuteil "Information" Jedes mal wenn du etwas änderst musst du mit Apply bestätigen.Felder die ich nicht erwähne lässt du so wie sie sind.

c.Im Menu "IP Settings" änderst du die IP Adresse auf 192.168.2.227. Nach" Apply" kannst du die LAN Verbindung trennen (und deaktivieren).

4. Jetzt lass den AP so stehen und aktiviere die WLAN Verbindung. Stelle die Verbindung zum Speedport her und gehe in das Konfigmenü des Gerätes rein. Im Menu "Netzwerk" aktiviere den Repeater Punkt. Trage die MAC Adresse des Netgears ein.

Das müsste alles sein.
Fragen?

Zitieren

26.10.2006, 13:54 — #5 (permalink)

Mediterror - offline
Neuer Benutzer
(Threadstarter)

Registriert seit: 25.10.2006
Ort: Fürth
Beiträge: 4

soweit ok teste es gleich mal aus. und wie "verbinde" ich meinen Laptop mit dem Netgear?

Zitieren

26.10.2006, 13:58 — #6 (permalink)

TinkyWinky - offline
CHIP-Spezialist für Netzwerke

Registriert seit: 29.11.2002
Ort: in der Pampa
Beiträge: 47.060

Per Netzwerkkabel.

Zitieren

26.10.2006, 14:14 — #7 (permalink)

Mediterror - offline
Neuer Benutzer
(Threadstarter)

Registriert seit: 25.10.2006
Ort: Fürth
Beiträge: 4

ich möchte ihn doch auch per wlan ansteuern.

Zitieren

26.10.2006, 14:16 — #8 (permalink)

TinkyWinky - offline
CHIP-Spezialist für Netzwerke

Registriert seit: 29.11.2002
Ort: in der Pampa
Beiträge: 47.060

Hast du meinen Beitrag gelesen und verstanden?

Zitieren

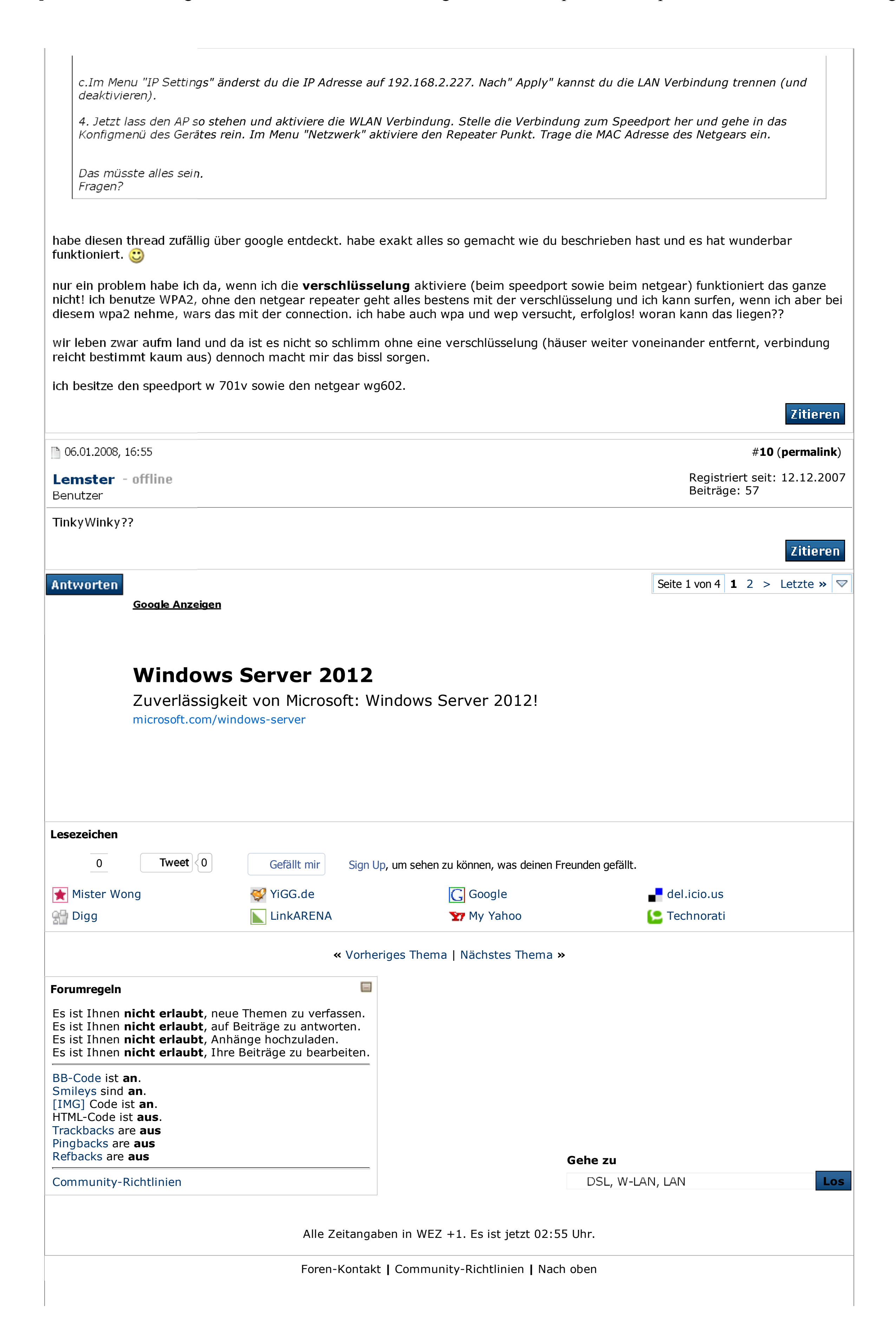
02.01.2008, 12:29 — #9 (permalink)

Lemster - offline
Benutzer

Registriert seit: 12.12.2007
Beiträge: 57

Zitat:

> Zitat von **TinkyWinky**
> *Rein theoretisch funktioniert es so:*
>
> *1. Zuerst musst du deinen PC per Kabel mit dem AP verbinden. Nur diese LAN Verbindung sollte aktiv sein, alle anderen deaktivieren. Stelle den AP irgenwo in der Nähe des Routers hin. Schalte im Router die Verschlüsselung aus. Auch MAC Filter sollte ggf. deaktiviert werden. SSID soll sichtbar sein.*
>
> *2. In den TCP/IP Eigenschaften der LAN Verbindung auf dem PC musst du eine IP manuell einragen. Welcher WG602 ist es? Wenn das ein WG 602v3 ist hat er die IP 192.168.1.227. Du musst also eine IP in diesem Bereich zuweisen. Nimm z.B. 192.168.1.222. Gateway und DNS ist hier egal, kann leer bleiben.*
>
> *3. Jetzt öffnest du einen Browser und tippst 192.168.1.227 ein. Im Konfigmenu machst du folgendes:*
>
> *a. Im Menu wireless Bridging stellst du "Repeater with Wireless Client Association" ein und trägst die MAC deines WLAN Routers ein. Die MAC Adresse findest du auf dem Typenschild beim Speedport. Mit "Apply" aktivierst du die Einstellung*
>
> *b. In "Wireless Settings" trägst du die SSID ein die im Speedport eingetragen ist. Auch derselbe Kanal wie im Speedport muss eingetragen werden. Falls du die Werte nicht auswendig kennst notiere dir das bevor du mit der Einrichtung startest. Notiere dir auch die MAC Adresse des Netgears. Diese findest du ganz oben im Menuteil "Information" Jedes mal wenn du etwas änderst musst du mit Apply bestätigen.Felder die ich nicht erwähne lässt du so wie sie sind.*



> *c.Im Menu "IP Settings" änderst du die IP Adresse auf 192.168.2.227. Nach" Apply" kannst du die LAN Verbindung trennen (und deaktivieren).*
>
> *4. Jetzt lass den AP so stehen und aktiviere die WLAN Verbindung. Stelle die Verbindung zum Speedport her und gehe in das Konfigmenü des Gerätes rein. Im Menu "Netzwerk" aktiviere den Repeater Punkt. Trage die MAC Adresse des Netgears ein.*
>
> *Das müsste alles sein.*
> *Fragen?*

habe diesen thread zufällig über google entdeckt. habe exakt alles so gemacht wie du beschrieben hast und es hat wunderbar funktioniert.

nur ein problem habe ich da, wenn ich die **verschlüsselung** aktiviere (beim speedport sowie beim netgear) funktioniert das ganze nicht! ich benutze WPA2, ohne den netgear repeater geht alles bestens mit der verschlüsselung und ich kann surfen, wenn ich aber bei diesem wpa2 nehme, wars das mit der connection. ich habe auch wpa und wep versucht, erfolglos! woran kann das liegen??

wir leben zwar aufm land und da ist es nicht so schlimm ohne eine verschlüsselung (häuser weiter voneinander entfernt, verbindung reicht bestimmt kaum aus) dennoch macht mir das bissl sorgen.

ich besitze den speedport w 701v sowie den netgear wg602.

Zitieren

06.01.2008, 16:55 #**10** (**permalink**)

Lemster - offline
Benutzer
Registriert seit: 12.12.2007
Beiträge: 57

TinkyWinky??

Zitieren

Antworten Seite 1 von 4 **1** 2 > Letzte »

Lesezeichen

0 Tweet 0 Gefällt mir Sign Up, um sehen zu können, was deinen Freunden gefällt.

Mister Wong | YiGG.de | Google | del.icio.us
Digg | LinkARENA | My Yahoo | Technorati

« Vorheriges Thema | Nächstes Thema »

Forumregeln

Es ist Ihnen **nicht erlaubt**, neue Themen zu verfassen.
Es ist Ihnen **nicht erlaubt**, auf Beiträge zu antworten.
Es ist Ihnen **nicht erlaubt**, Anhänge hochzuladen.
Es ist Ihnen **nicht erlaubt**, Ihre Beiträge zu bearbeiten.

BB-Code ist **an**.
Smileys sind **an**.
[IMG] Code ist **an**.
HTML-Code ist **aus**.
Trackbacks are **aus**
Pingbacks are **aus**
Refbacks are **aus**

Community-Richtlinien

Gehe zu
DSL, W-LAN, LAN Los

Alle Zeitangaben in WEZ +1. Es ist jetzt 02:55 Uhr.

Foren-Kontakt | Community-Richtlinien | Nach oben

Überblick Beliebteste Produkte Mobil Archiv Foren-Archiv Beliebteste Themen Neueste Themen RSS

Impressum Nutzungshinweis Datenschutz Presse Jobs Mediadaten Über unsere Werbung CHIP-Kiosk Abo

Kontakt

User’s Guide for the WG602 v3 54 Mbps Wireless Access Point



NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA
Phone 1-888-NETGEAR

202-10060-01
September 2004

NETGEAR, INC.

Technical Support

Please register to obtain technical support. Please retain your proof of purchase and warranty information.

To register your product, get product support or obtain product information and product documentation, go to *www.netgear.com*. If you do not have access to the World Wide Web, you can register your product by filling out the registration card and mailing it to NETGEAR customer service.

You will find technical support information at:
www.netgear.com/support/main.asp through the customer service area. If you want to contact technical support by telephone, see the support information card for the correct telephone number for your country.

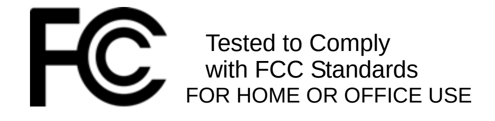
Trademarks

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

NETGEAR 54 Mbps Wireless Access Point WG602 v3



Warning!

To comply with the FCC's exposure requirements you must maintain a distance of at least 1 cm from the antenna of this device while it is in use. This device should not be co-located with other transmitters.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help.

RF Exposure Requirements

WARNING! To ensure compliance with FCC RF exposure requirements, the antenna used for this device must be installed to provide a separation distance of at least 20 cm (8 in) from all persons and must not be co-located or operating in conjunction with any other antenna or radio transmitter. Installers and end-users must follow the installation instructions provided in this user guide.

Radio Frequency Interference Requirements

This device is restricted to indoor use due to its operation in the 2.4 GHz frequency range. FCC requires this product to be used indoors in 2.4 GHz the frequency range to reduce the potential for harmful interference to co-channel Mobile Satellite systems.

Regulatory Compliance Information

This device is restricted to indoor use due to reduce the potential for harmful interference to co-channel Mobile Satellite and Radar Systems.

Canadian Department of Communications Compliance Statement

This Class B Digital apparatus (54 Mbps Wireless Access Point WG602 v3) meets all the requirements of the Canadian Interference Causing Equipment Regulations.

Cet appareil numerique del la classe B respect les exigences du Regalement sur le material broilleur du Canada.

This device comples with Class B limits of Industry of Canada. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

The device is certified to the requirements of RSS-139-1 and RSS-210 for 2.4 GHz spread spectrum devices. The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations. For further information, contact your local Industry Canada office.

CE Declaration of Conformity

For the following equipment: 54 Mbps Wireless Access Point WG602 v3

CE 0984 ⓘ

is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility (89/336/EEC), Low-voltage Directive (73/23/EEC) and the Amendment Directive (93/68/EEC), the procedures given in European Council Directive 99/5/EC and 89/3360EEC. The equipment was passed. The test was performed according to the following European standards:

- EN 301489-1 V1.2.1 (2000-08)
- EN 301 489-17 V1.1.1 (2000-09)
- EN60950 / EN300328

Contents

Appendix B
Wireless Networking Basics

Appendix C
Network, Routing, Firewall, and Cabling Basics

Chapter 1
About This Manual

This chapter introduces the conventions and features of this document.

Audience, Scope, Conventions

This manual assumes that the reader has basic to intermediate computer and Internet skills. However, tutorial information is provided in the Appendices, on the *Resource CD for the 54 Mbps Wireless Access Point WG602 v3 (230-10106-01)*, and on the NETGEAR Web site.

This manual uses the following typographical conventions:

Table 1. Typographical conventions

italics	Emphasis.
bold	User input.
[Enter]	Named keys in text are shown enclosed in square brackets.
SMALL CAPS	DOS file and directory names.

This manual uses the following formats to highlight special messages:



Note: This format is used to highlight information of importance or special interest.

This manual is written according to these specifications:

Table 1-1. Manual Specifications

Product Version	54 Mbps Wireless Access Point WG602 v3
Manual Part Number	202-10060-01
Manual Publication Date	September 2004



Note: Product updates are available on the NETGEAR Web site at *http://kbserver.netgear.com/products/WG602v3.asp*.

How to Use this Manual

The HTML version of this manual includes these features.

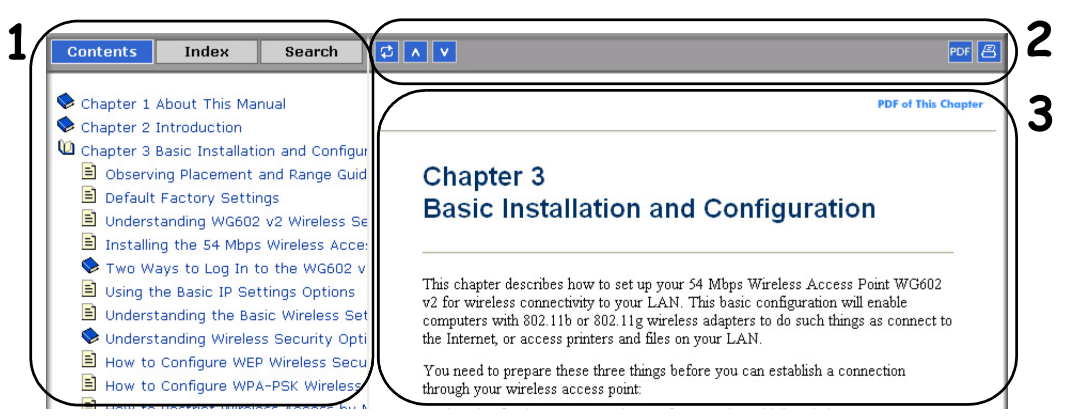


Figure 1-1: HTML version of this manual

1. **Left pane**. Use the left pane to view the Contents, Index, Search, and Favorites tabs.

   To view the HTML version of the manual, you must have a version 4 or later browser with JavaScript enabled.

2. **Toolbar buttons**. Use the toolbar buttons across the top to navigate, print pages, and more.

   The *Show in Contents* button locates the current topic in the Contents tab.

   The Previous/Next buttons display the previous or next topic.

   PDF — The *PDF* button links to a PDF version of the full manual.

   The *Print* button prints the current topic. Using this button when a step-by-step procedure is displayed will send the entire procedure to your printer--you do not have to worry about specifying the correct range of pages.

3. **Right pane**. Use the right pane to view the contents of the manual. Also, each page of the manual includes a **PDF of This Chapter** link at the top right which links to a PDF file containing just the currently selected chapter of the manual.

How to Print this Manual

To print this manual you man choose one of the following several options, according to your needs.

- **Printing a "How To" Sequence of Steps in the HTML View**. Use the *Print* button on the upper right of the toolbar to print the currently displayed topic. Using this button when a step-by-step procedure is displayed will send the entire procedure to your printer--you do not have to worry about specifying the correct range of pages.
- **Printing a Chapter**. Use the PDF of This Chapter link at the top right of any page.
  - Click "PDF of This Chapter" link at the top right of any page in the chapter you want to print. A new browser window opens showing the PDF version of the chapter you were viewing.
  - Click the print icon in the upper left of the window.
  - **Tip**: If your printer supports printing two pages on a single sheet of paper, you can save paper an printer ink by selecting this feature.
- **Printing the Full Manual**. Use the PDF button in the toolbar at the top right of the browser window.
  - Click PDF button. A new browser window opens showing the PDF version of the chapter you were viewing.
  - Click the print icon in the upper left of the window.
  - **Tip**: If your printer supports printing two pages on a single sheet of paper, you can save paper an printer ink by selecting this feature.

Chapter 2
Introduction

This chapter introduces the NETGEAR 54 Mbps Wireless Access Point WG602 v3. Minimal prerequisites for installation are presented in “System Requirements” on page 2-3.

About the 54 Mbps Wireless Access Point WG602 v3

The 54 Mbps Wireless Access Point WG602 v3 is the basic building block of a wireless LAN infrastructure. It provides connectivity between wired Ethernet networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices.

The WG602 v3 provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage, interacting with a wireless network interface card (NIC) via an antenna. Typically, an in-doors access point provides a maximum connectivity area with about a 300 foot radius. The 54 Mbps Wireless Access Point WG602 v3 can support a small group of users in a range of several hundred feet. Most access points are rated for up to 32 users simultaneously.

The auto-sensing capability of the 54 Mbps Wireless Access Point WG602 v3 allows packet transmission at up to 54 Mbps, or at reduced speeds to compensate for distance or electromagnetic noise interference.

Support for Standards

The following standards and conventions are supported:

- **Standards Compliant.** The WG602 v3 Access Point complies with the IEEE 802.11g (DSSS).
- **WEP support.** Support for WEP is included. Both 64-bit and 128-bit keys are supported.
- **WPA-PSK support**. Support for Wi-Fi Protected Access (WPA) data encryption which provides strong data encryption and authentication based on a pre-shared key.
- **Dynamic WEP key Support.** Fixed or Dynamic WEP (Wired Equivalent Privacy) keys can be used.
- **DHCP Client Support.** DHCP provides a dynamic IP address to PCs and other devices upon request. The WG602 v3 can act as a client and obtain information from your DHCP server.

- **NetBIOS & WINS Support.** Support for both NetBIOS broadcast and WINS (Windows Internet Naming Service) allows the WG602 v3 to easily fit into your existing Windows network.

Key Features

The WG602 v3 provides solid functionality, including these features:

- **Wireless Access Point.** Operates as a standard 802.11g access point.
- **Wireless Bridging.** Operates as a point-to-point or multi-point wireless bridge.
- **Upgradeable Firmware.** Firmware is stored in a flash memory and can be upgraded easily, using only your Web browser, and can be upgraded remotely.
- **Access Control.** The Access Control MAC Address filtering feature can ensure that only trusted wireless stations can use the WG602 v3 to gain access to your LAN.
- **Simple Configuration.** If the default settings are unsuitable, they are easy to change.
- **Hidden Mode.** The SSID is not broadcast, assuring only clients configured with the correct SSID can connect.
- **Autosensing Ethernet Connection with Auto Uplink Interface.** Connects to 10/100 Mbps IEEE 802.3 Ethernet networks.
- **LED Indicators.** Power and wireless activity are easily identified.

802.11g Standards-based Wireless Networking

The 54 Mbps Wireless Access Point WG602 v3 provides a bridge between Ethernet wired LANs and 802.11g compatible wireless LAN networks. It provides connectivity between Ethernet wired networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices. Additionally, the WG602 v3 supports the following wireless features:

- Distributed coordinated function (CSMA/CA, Back off procedure, ACK procedure, retransmission of unacknowledged frames)
- RTS/CTS handshake
- Beacon generation
- Packet fragmentation and reassembly
- Authentication Algorithms (Open System, Shared Key, WPA-PSK)
- Short or long preamble
- Roaming among access points on the same subnet

Autosensing Ethernet Connections with Auto Uplink

The WG602 v3 can connect to a standard Ethernet network. The LAN interface is autosensing and capable of full-duplex or half-duplex operation. The wireless access point incorporates Auto Uplink™ technology. The Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a 'normal' connection such as to a PC or an 'uplink' connection such as to a switch or hub. That port will then configure itself to the correct configuration. This feature also eliminates any concerns about crossover cables, as Auto Uplink will accommodate either type of cable to make the right connection.

Compatible and Related NETGEAR Products

For a list of compatible products from other manufacturers, see the Wireless Ethernet Compatibility Alliance Web site (WECA, see *http://www.wi-fi.net*).

The following NETGEAR products work with the WG602 v3 Access Point:

- WAB501 a/b Dual Band Wireless PC Card Adapter
- MA401 802.11b Wireless PC Card
- WG511 802.11g Wireless CardBus Adapter
- MA111 802.11b Wireless USB Adapter
- MA311 802.11b Wireless PCI Adapter
- MA701 802.11b Wireless Compact Flash Card
- WAG511 802.11a/g Wireless CardBus Adapter
- MA701 802.11b Compact Flash Wireless Adapter
- WGE101 802.11g Wireless Bridge
- WG311 802.11g Wireless PCI Adapter
- WAG311 802.11a/g Wireless PCI Adapter

System Requirements

Before installing the WG602 v3, make sure your network meets these requirements:

- A hub, switch, or Cable/DSL router with an available 10/100 Mbps Ethernet port
- A Category 5 UTP straight through Ethernet cable with RJ-45 connector included in the package, or one like it
- A 100-240 V, 50-60 HZ AC power source
- A Web browser for configuration such as Microsoft Internet Explorer 5.0 or above, or Netscape Navigator 4.78 or above

- At least one Pentium class computer (or equivalent) with the TCP/IP protocol installed
- Other 802.11b or 802.11g-compliant devices

What's In the Box?

The product package should contain the following items:

- 54 Mbps Wireless Access Point WG602 v3
- Power adapter and cord (12Vdc, 1.2A)
- Straight through Category 5 Ethernet cable—10 feet (3.04 m)
- Printed 54 Mbps Wireless Access Point WG602 v3 Quick Installation Guide
- *Resource CD for the 54 Mbps Wireless Access Point WG602 v3 (230-10106-01)*
  – User's Guide for the WG602 v3 54 Mbps Wireless Access Point (202-10060-01)—this manual
  – Windows TCP/IP and Networking Tutorials
  – Animated Install Assistant
  – Soft copy of the 54 Mbps Wireless Access Point WG602 v3 Quick Installation Guide
- Support Information card
- Warranty and Registration card

Contact your reseller or customer support in your area if there are any wrong, missing, or damaged parts. You can refer to the Support Information Card for the telephone number of customer support in your area. You should keep the Support Information card, along with the original packing materials, and use the packing materials to repack the WG602 v3 if you need to return it for repair. To qualify for product updates and product warranty registrations, we encourage you to register on the NETGEAR Web site at: *http://www.netgear.com*.

Hardware Description

The 54 Mbps Wireless Access Point WG602 v3 front and rear hardware functions are described below.

WG602 v3 Wireless Access Point Front Panel

The WG602 v3 Access Point provides three status LEDs.

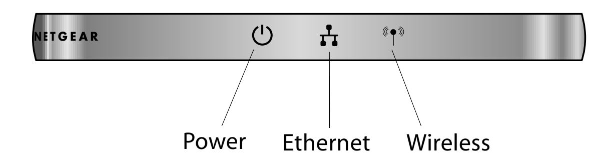


Figure 2-1: WG602 v3 front panel

The following table explains the LED indicators:

LED	DESCRIPTION
Power	Power Indicator
Off	No power. If this LED does not come on with the power adapter and cord correctly installed, see Chapter 6, "Troubleshooting."
On	Power is on.
Ethernet	Ethernet LAN Link Activity Indicator
Off	Indicates no Ethernet link detected.
Green On	100 Mbps Fast Ethernet link detected, no activity.
Green Blink	Indicates data traffic on the 100Mbps Ethernet LAN.
Amber 0n	10 Mbps Ethernet link detected, no activity.
Amber Blink	Indicates data traffic on the 10Mbps Ethernet LAN.
Wireless	Wireless LAN Link Activity Indicator
Off	Indicates no wireless link detected.
Green On	Wireless link enabled, no activity.
Green Blink	Wireless link activity.

WG602 v3 Wireless Access Point Rear Panel

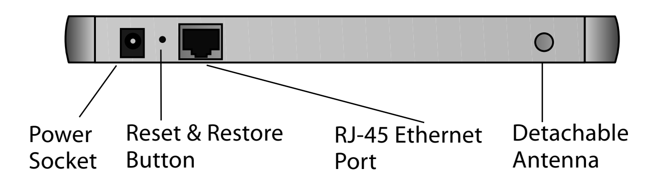


Figure 2-2: WG602 v3 rear panel

Power Socket

This socket connects to the WG602 v3 power adapter.

Reset and Restore to Factory Defaults Button

The reset and restore to defaults button located between the Ethernet RJ-45 connector and the power socket resets the WG602 v3 when pushed once or restores to the factory default settings when pushed and held for 10 seconds.

RJ-45 Ethernet Port

Use the WG602 v3 Ethernet RJ-45 port to connect to an Ethernet LAN through a device such as a hub, switch, or router.

Detachable Antenna

The WG602 v3 provides a detachable antenna. Be sure the antenna is securely fastened.

Chapter 3
Basic Installation and Configuration

This chapter describes how to set up your 54 Mbps Wireless Access Point WG602 v3 for wireless connectivity to your LAN. This basic configuration will enable computers with 802.11b or 802.11g wireless adapters to do such things as connect to the Internet, or access printers and files on your LAN.

You need to prepare these three things before you can establish a connection through your wireless access point:

- A location for the WG602 v3 that conforms to the guidelines below.
- A device such as a hub, switch, router, or Cable/DSL gateway.
- One or more computers with properly configured 802.11b or 802.11g wireless adapters.

Observing Placement and Range Guidelines

	**Note:** Indoors, computers can connect over wireless networks at ranges of several hundred feet or more. This distance can allow for others outside your area to access your network. It is important to take appropriate steps to secure your network from unauthorized access. The WG602 v3 Access Point provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the wireless access point. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices.

	**Note:** Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the WG602 v3.

For best results, place your wireless access point:

- Near the center of the area in which your PCs will operate.
- In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls).
- Away from sources of interference, such as PCs, microwaves, and 2.4 GHz cordless phones.
- Away from large metal surfaces.
- If using multiple access points, it is better if adjacent access points use different radio frequency Channels to reduce interference. The recommended Channel spacing between adjacent access points is 5 Channels (for example, use Channels 1 and 6, or 6 and 11).

The time it takes to establish a wireless connection can vary depending on both your security settings and placement.

Default Factory Settings

When you first receive your WG602 v3, the default factory settings will be set as shown below. To restore these defaults, see "WG602 v3 Wireless Access Point Rear Panel" on page 2-6.

FEATURE	FACTORY DEFAULT SETTINGS
User Name (case sensitive)	**admin**
Password (case sensitive)	**password**
Access Point Name	**NETGEARxxxxxx where xxxxxx are the last six digits of the wireless access point's MAC address**
DHCP	**DHCP client**
IP Configuration if DHCP server is unavailable	**IP Address: 192.168.0.227** **Subnet Mask: 255.255.255.0** **Gateway: 0.0.0.0**
Wireless Mode (Access Point or Bridge)	**Access Point**
Wireless Network Name (SSID)	**NETGEAR**
Broadcast Network Name	**Enabled**
802.11g/b Radio Frequency Channel	**11**
WEP/WPA	**Disabled**
Authentication Type	**Auto**

Understanding WG602 v3 Wireless Security Options

Unlike wired network data, your wireless data transmissions can be received well beyond your walls by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The WG602 v3 Access Point provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

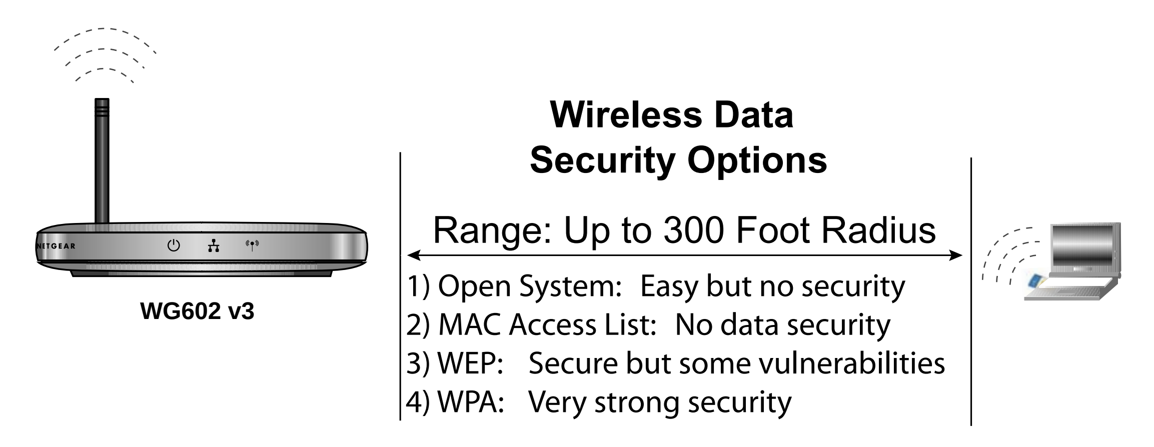


Figure 3-1: WG602 v3 wireless data security options

There are several ways you can enhance the security of your wireless network:

- **Restrict Access Based on MAC Address.** You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the WG602 v3. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
- **Turn Off the Broadcast of the Wireless Network Name (SSID).** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network 'discovery' feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers.
- **Use WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption will block an eavesdropper but because the keys are static, a determined snoop can learn the keys in less than a day of eavesdropping.
- **Use WPA-PSK.** Wi-Fi Protected Access (WPA) data encryption provides data security. WPA-PSK will block eavesdropping. Because this is a new standard, wireless device driver and software availability may be limited. However, WPA is not available in bridge mode.

Installing the 54 Mbps Wireless Access Point WG602 v3

Follow the instructions below to set up and test basic wireless connectivity. Once you have established basic wireless connectivity, you can enable security settings and configure the advanced wireless functions.

Before installing the 54 Mbps Wireless Access Point WG602 v3, you should make sure that your Ethernet network is up and working. You will be connecting the access point to the Ethernet network so that computers with 802.11b or 802.11g wireless adapters will be able to communicate with computers on the Ethernet network. In order for this to work correctly, verify that you have met all of the system requirements, shown on page 2-3.

1 Set up the WG602 v3 Access Point

Tip: Before mounting the WG602 v3 in a high location, first set up and test the WG602 v3 to verify wireless network connectivity.

a. Prepare a PC with an Ethernet adapter. If this PC is already part of your network, record its TCP/IP configuration settings.

b. Configure the PC with a static IP address of 192.168.0.210 and 255.255.255.0 for the Subnet Mask.

c. Connect an Ethernet cable from the WG602 v3 to the PC (**A)**.

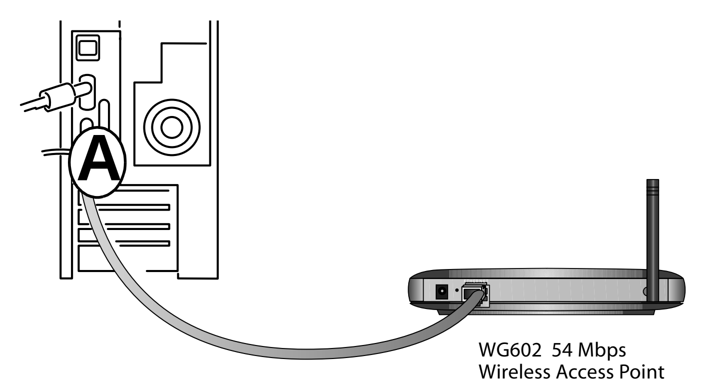


Figure 3-2: Set up the WG602 v3

d. Turn on your computer, connect the power adapter to the WG602 v3 and verify the following:



The power light goes on.

The LAN light of the wireless access point is lit when connected to a powered on PC.

2 Configure LAN and Wireless Access

The WG602 Wireless Access Point can be configured remotely from Microsoft Internet Explorer browser version 5.0 or above, or Netscape Navigator web browser version 4.78 or above on your computer.

1. The WG602 v3 is set by default to be a DHCP client. So, if the WG602 v3 has not yet been installed, and there is no DHCP server on the network, you can log in to the WG602 v3 using its default IP address. 192.168.0.227 is the default IP address of your access point.

   Note: This procedure which uses a static IP configuration. If WG602 v3 has already been installed or it is connected to a network where there as a DHCP server as commonly found in home routers, you can the NetBIOS login described in "How to Log In to the WG602 v3 Using Its Default NetBIOS Name" on page 3-9.
2. Open a Web browser such as Internet Explorer or Netscape Navigator.
3. Connect to the WG602 v3 by entering its default address of *http://192.168.0.227* into your browser.



e. A login window like the one shown below opens:

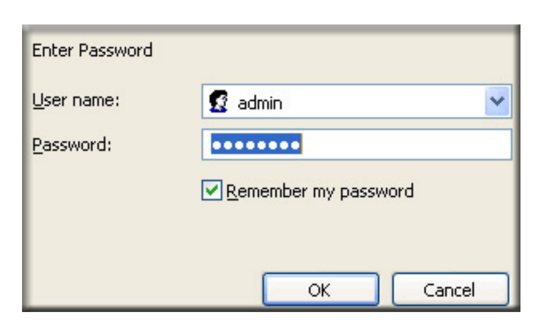


Figure 3-3: Login window

– When prompted, enter **admin** for the user name and **password** for the password, both in lower case letters.
– Click **IP Settings** and configure the IP Settings according to your network setup.

f. Configure the wireless interface for wireless access. See the online help or the "Understanding the Basic Wireless Settings" on page 3-11 for full instructions.

Note: You must set the Regulatory Domain. It may not be legal to operate the wireless access point in a region other than one of those identified in this field.

Now that you have finished the setup steps, you are ready to deploy the WG602 v3 in your network. If needed, you can now reconfigure the PC you used in step 1 back to its original TCP/IP settings.

3 Deploy the WG602 v3 Access Point

a. Disconnect the WG602 v3 and position it where you will deploy it. The best location is elevated at the center of your wireless coverage area.

b. Lift the antenna side so that it is vertical.

c. Connect an Ethernet cable from your WG602 v3 Access Point to a LAN port on your router, switch, or hub.

   Note: By default, WG602 v3 is set to be a DHCP client. If your network uses static IP addresses, you will need to change this setting.

d. Connect the power adapter to the wireless access point and plug the power adapter in to a power outlet. The power, LAN, and wireless lights and should light up.

4 Verify Wireless Connectivity

Using a computer with an 802.11b or 802.11g wireless adapter with the correct wireless settings needed to connect to the WG602 v3 (SSID, MAC ACL, WEP, WPA, etc.), verify connectivity by using a browser such as Netscape or Internet Explorer to browse the Internet, or check for file and printer access on your network. If you cannot connect, see "Troubleshooting" on page 6-1.

Two Ways to Log In to the WG602 v3

The 54 Mbps Wireless Access Point WG602 v3 can be configured remotely from Microsoft Internet Explorer browser version 5.0 or above, or Netscape Navigator Web browser version 4.78 or above. You can log in to the WG602 v3 in these two ways:

- Using the Default IP Address of the WG602 v3 is the most reliable.
- Using the NetBIOS name of the WG602 v3 is not as reliable as using the IP Address.

The procedures for these two ways of logging in to the WG602 v3 are presented here.

How to Log in Using the Default IP Address of the WG602 v3

1. 192.168.0.227 is the default IP address of your access point. However, the WG602 v3 is also set, by default, to be a DHCP client. So, if the WG602 v3 has not yet been installed, and there is no DHCP server on the network, you can log in to the WG602 v3 using its default IP address. Otherwise, you should use either the NetBIOS login described in "How to Log In to the WG602 v3 Using Its Default NetBIOS Name" on page 3-9 or the procedure described in "Set up the WG602 v3 Access Point" on page 3-4" which uses a static IP configuration.

   Note: The computer you are using to connect to the WG602 v3 should be configured with an IP address that starts with 192.168.0.x and a Subnet Mask of 255.255.255.0.
2. Open a Web browser such as Internet Explorer or Netscape Navigator.
3. Connect to the WG602 v3 by entering its default address of *http://192.168.0.227* into your browser.



4. A login window like the one shown below opens:



Figure 3-4: Login window

Log in use the default user name of **admin** and default password of **password**.

Once you have entered your access point name, your Web browser should automatically find the WG602 v3 Access Point and display the home page, as shown in "Login result: WG602 v3 home page" on page 3-8.

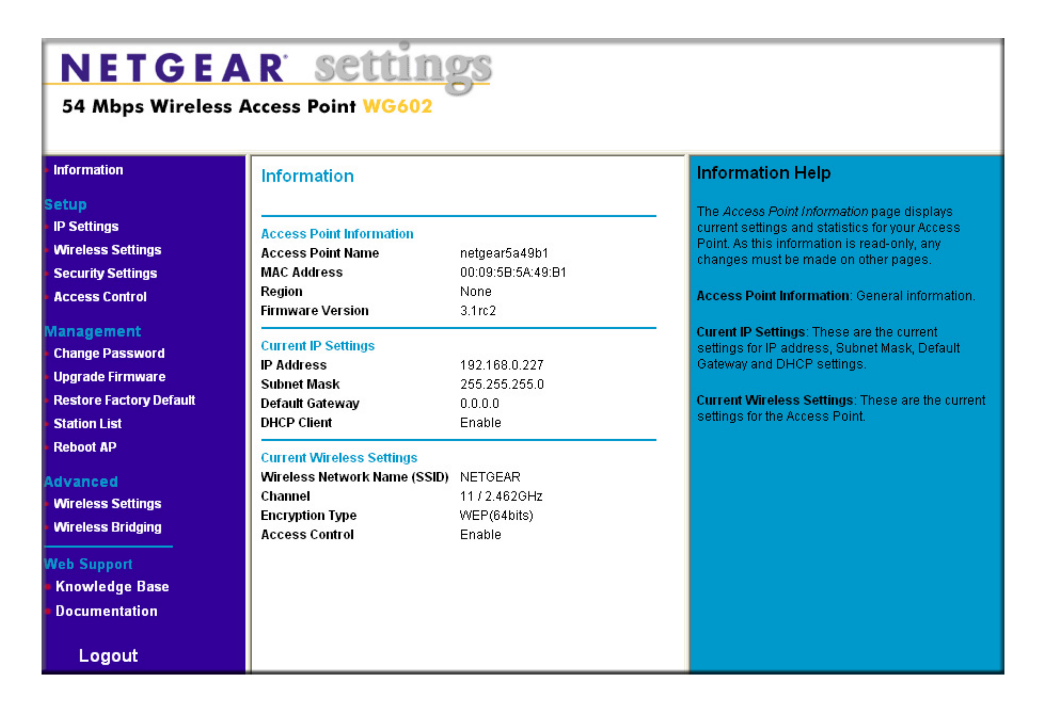


Figure 3-5: Login result: WG602 v3 home page

The browser will then display the WG602 v3 settings home page.

When the wireless access point is connected to the Internet, click the Knowledge Base or the Documentation link under the Web Support menu to view support information or the documentation for the wireless access point.

If you do not click Logout, the wireless access point will wait 5 minutes after there is no activity before it automatically logs you out.

How to Log In to the WG602 v3 Using Its Default NetBIOS Name

The 54 Mbps Wireless Access Point WG602 v3 can be configured remotely from Microsoft Internet Explorer browser version 5.0 or above, or Netscape Navigator Web browser version 4.78 or above. You can connect to the WG602 v3 by using its default NetBIOS name or its default IP address. The instructions for connecting using the default NetBIOS name are below. The instructions for connecting using the default IP address follow this section.

1. Determine the NetBIOS name of your access point.

   To find the NetBIOS name, refer to the labels on the bottom of your access point. The access point NetBIOS name is formed from the word "NETGEAR" and last 6 digits of the access point's MAC address on the label on the bottom of the unit. It is formatted like "NETGEAR123456" with no spaces or delimiters.

   Note: If the computer you are using to connect to the WG602 v3 is on a different subnet, you will not be able to connect via its NetBIOS name unless there is a WINS server on your LAN. If the NetBIOS name login fails, use the procedure for "How to Log in Using the Default IP Address of the WG602 v3" on page 3-7.

2. Open a Web browser such as Internet Explorer or Netscape Navigator.
3. Log in to the WG602 v3 using the NetBIOS name you found on the bottom of the unit.

   In this example, you see NETGEAR123456 in the browser address or location box. There is no space between "NETGEAR" and the 6 digits of the access point name.You do not need to include "www" or "http://."

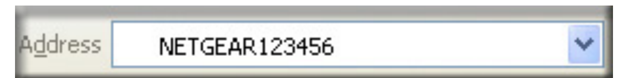


Figure 3-6: Example WG602 v3 NetBIOS name in browser address bar

4. A login window like the one shown below opens:

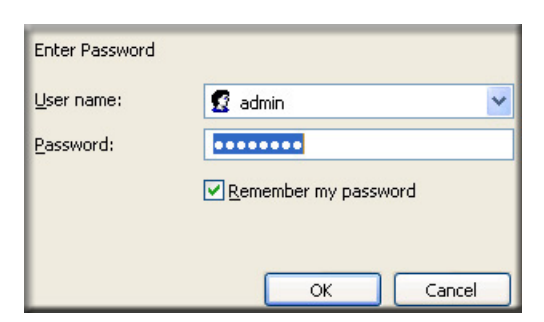


Figure 3-7: Login window

Enter the default user name of **admin** and the default password of **password**.

Using the Basic IP Settings Options

The IP Settings page is under the Setup heading of the main menu. Use this page to configure DHCP, static IP, and the access point NetBIOS name.

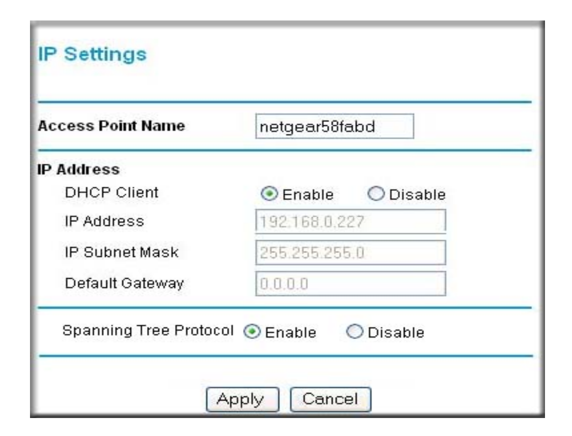


Figure 3-8: Basic IP Settings page

- **Access Point Name (NetBIOS)**
  You can change the access point name after the initial configuration. Enter a new name for the wireless access point and click Apply to save your changes.
- **The IP Address Source**
  The wireless access point is shipped preconfigured to use a private IP address on the LAN side, and to act as a DHCP client. If the wireless access point does not find a DHCP server on the Ethernet LAN, it defaults to this IP configuration:
  - DHCP Client - *Enable*
  - IP Address — 192.168.0.227
  - IP Subnet Mask — 255.255.255.0
  - Gateway — 0.0.0.0

  If your network has a requirement to use a different IP addressing scheme, you can make those changes in this page.
- **Spanning Tree Protocol**
  Spanning Tree Protocol in enabled by default for the wireless access point. This provides network traffic optimization in settings with multiple WG602 v3 Access Points.

Remember to click **Apply** to save your changes.

Understanding the Basic Wireless Settings

To configure the wireless settings of your wireless access point, click the Wireless Settings link in the Setup section of the main menu of the browser interface. The Wireless Settings page appears, as shown below.

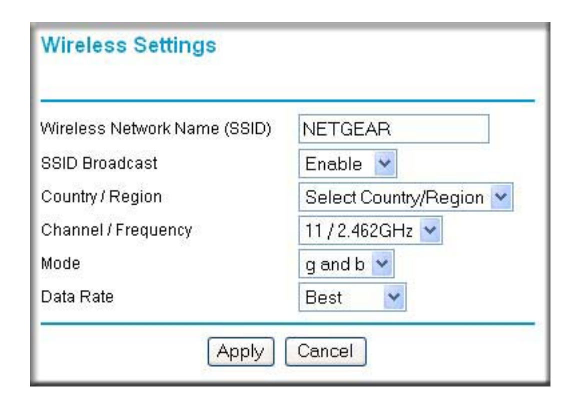


Figure 3-9: Basic Wireless Settings page

The Basic Wireless Settings options are discussed below:

- **Wireless Network Name (SSID).** The SSID is also known as the wireless network name. Enter a value of up to 32 alphanumeric characters; the characters are case sensitive. In a setting where there is more than one wireless network, different wireless network names provide a means for separating the traffic. Any device you want to participate in a particular wireless network needs to use the SSID. The WG602 v3 default SSID is: **NETGEAR**.

  Note: Different access points within an area can use different channels. To reduce interference, adjacent access points *should* use different channels.

- **SSID Broadcast.** The default is Enable. If SSID Broadcast is disabled, only devices that have the correct SSID can connect.
- **Country/Region.** This field identifies the region where the WG602 v3 can be used. It may not be legal to operate the wireless features of the wireless access point in a region other than one of those identified in this field. There is no default country region, and the channel is set to 11. Unless a region is selected, the channel cannot be changed.

- **Channel/Frequency.** This field identifies which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems or setting up the WG602 v3 near another access point. See "Wireless Channels" on page B-2 for more information on wireless channels.
  - Access points use a fixed channel. You can select the channel used. This allows you to choose a channel which provides the least interference and best performance. In the USA and Canada, 11 channels are available.
  - If using multiple access points, it is better if adjacent access points use different channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (for example, use channels 1 and 6, or 6 and 11).
  - In "Infrastructure" mode, wireless stations normally scan all channels, looking for an access point. If more than one access point can be used, the one with the strongest signal is used. This can only happen when the various access points are using the same SSID.
- **Mode.** The default is g and b. You can change the mode to g or b only.
- **Data Rate.** Shows the available transmit data rate of the wireless network. The possible data rates supported are: 1 Mbps, 2 Mbps, 5.5 Mbps, 6 Mbps, 9 Mbps, 11 Mbps, 12 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, 54 Mbps, and Best.The default is Best.

Understanding Wireless Security Options

The table below identifies the various basic wireless security options. A full explanation of these standards is available in Appendix B, "Wireless Networking Basics".

Table 3-1. Basic Wireless Security Options

Field	Description
Off	No wireless security.
WEP	WEP offers the following options: • Open System With Open Network Authentication and 64- or 128-bit WEP Data Encryption, the WG602 v3 *does* perform 64- or 128-bit data encryption but *does not* perform any authentication. • Shared Key Shared Key authentication encrypts the SSID and data. Choose the Encryption Strength (64- or 128-bit data encryption). Manually enter the key values or enter a word or group of printable characters in the Passphrase box. Manually entered keys *are* case sensitive but passphrase characters *are not* case sensitive. **Note**: Not all wireless adapter configuration utilities support passphrase key generation. • Auto
WPA-PSK	WPA-Pre-shared Key *does* perform authentication, uses 128-bit data encryption and dynamically changes the encryption keys making it nearly impossible to circumvent. Enter a word or group of printable characters in the Password Phrase box. These characters *are* case sensitive. **Note**: Not all wireless adapter configuration utilities support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA.

Information to Gather Before Changing Basic Wireless Settings

Before customizing your wireless settings, print this form and record the following information. If you are working with an existing wireless network, the person who set up or is responsible for the network will be able to provide this information. Otherwise, you will choose the settings for your wireless network. Either way, record the settings for your wireless network in the spaces below.

- **Wireless Network Name (SSID)*:*** ______________________________ The SSID, identifies the wireless network. You can use up to 32 alphanumeric characters. The SSID is case sensitive. The SSID in the wireless adapter card must match the SSID of the wireless access point. In some configuration utilities (such as in Windows XP), the term "wireless network name" is used instead of SSID.
- **If WEP Authentication is Used.** Circle one: **Open System**, **Shared Key, or Auto**.

  Note: If you select Shared Key, the other devices in the network will not connect unless they are set to Shared Key as well and are configured with the correct key.

  – **WEP Encryption key size**. Choose one: **64-bit** or **128-bit**. Again, the encryption key size must be the same for the wireless adapters and the wireless access point.

  – **Data Encryption (WEP) Keys**. There are two methods for creating WEP data encryption keys. Whichever method you use, record the key values in the spaces below.

    - **Passphrase method**. ______________________________ These characters *are* case sensitive. Enter a word or group of printable characters and click the Generate Keys button. Not all wireless devices support the passphrase method.
    - **Manual method**. These values *are not* case sensitive. For 64-bit WEP, enter 10 hex digits (any combination of 0-9 or a-f). For 128-bit WEP, enter 26 hex digits.

    Key 1: ___________________________________

    Key 2: ___________________________________

    Key 3: ___________________________________

    Key 4: ___________________________________

- **If WPA-PSK Authentication is Used.**

  – **Passphrase**: ______________________________ These characters *are* case sensitive. Enter a word or group of printable characters. When you use WPA-PSK, the other devices in the network will not connect unless they are set to WPA-PSK as well and are configured with the correct Passphrase.

Use the procedures described in the following sections to configure the WG602 v3. Store this information in a safe place.

How to Configure WEP Wireless Security

	**Note:** If you use a wireless PC to configure WEP settings, you will be disconnected when you click Apply. Reconfigure your wireless adapter to match the new settings or access the wireless access point from a wired PC to make any further changes.

To configure WEP data encryption, follow these steps:

1. Click the Security Settings link in the Setup section of the main menu and select WEP for the Security Type.

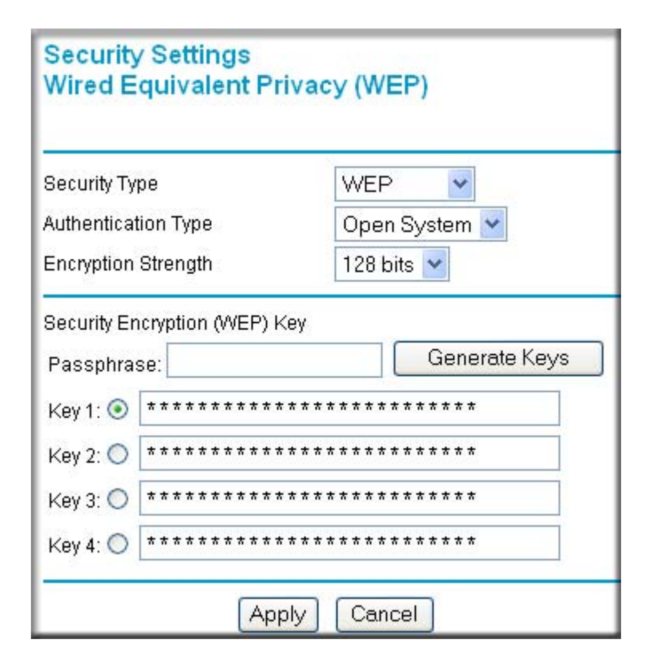


Figure 3-10: WEP Settings page

2. The Authentication Type is set to Any by default. Change the Authentication Type to Shared Key to use WEP data encryption.
3. For the Encryption Strength, select 64- or 128-bit encryption.
4. You can manually or automatically program the four data encryption keys. These values must be identical on all PCs and access points in your network.

- Automatic — enter a word or group of printable characters in the Passphrase box and click the Generate button. The four key boxes will be automatically populated with key values.
- Manual — enter ten hexadecimal digits (any combination of 0-9, a-f, or A-F) Select which of the four keys will be active.

See "WEP Wireless Security" on page B-4 for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard.

5. Click Apply to save your settings.

How to Configure WPA-PSK Wireless Security

Note: Not all wireless adapters support WPA. Furthermore, client software is also required. Windows XP and Windows 2000 with service pack 3 do include WPA support. Nevertheless, the wireless adapter hardware and driver must also support WPA. For instructions on configuring wireless PCs or PDAs for WPA-PSK security, consult the documentation for the product you are using.

To configure WPA-PSK, follow these steps:

1. Click the Security Settings link in the Setup section of the main menu and select WPA-PSK for the Security Type.



Figure 3-11: WPA Settings menu

2. Enter a word or group of 8-63 printable characters in the Password Phrase box.
3. Click Apply to save your settings.



Note: If you use a wireless PC to configure WPA settings, you will be disconnected when you click Apply. Reconfigure your wireless adapter to match the new settings or access the wireless access point from a wired PC to make any further changes.

How to Restrict Wireless Access by MAC Address

The Access Control page lets you block or allow the network access privilege of the specified stations through the 54 Mbps Wireless Access Point WG602 v3. This provides an additional layer of security.



Note: When configuring the WG602 v3 from a wireless PC whose MAC address is not in the access control list, if you select Turn Access Control On, you will lose your wireless connection when you click Apply. You must then access the wireless access point from a wired PC or from a wireless PC which is on the access control list to make any further changes.

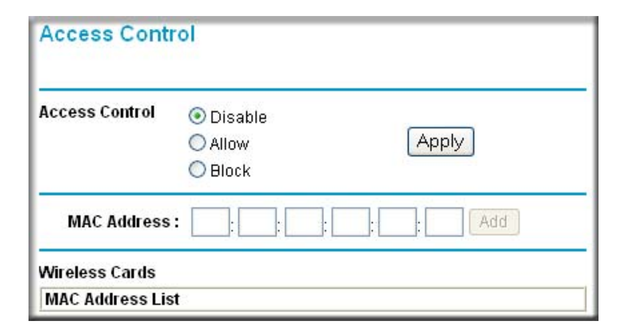


Figure 3-12: Access Control options

To restrict access based on MAC Addresses, follow these steps:

1. From the Setup section of the main menu, click Access Control to display the Wireless Access page shown below.
2. Select the type of Access Control:

- Disable
- Allow
- Block

3. Then, enter the MAC address for a device you plan to use. You can usually find the MAC address printed on the wireless adapter.

   You can copy and paste the MAC addresses from the WG602 v3's Station List page into the MAC Address box. To do this, configure each wireless PC to obtain a wireless link to the WG602 v3. The PC should then appear in the Station List page.

4. Click Add to add the wireless device to the access list. Repeat these steps for each additional device you want to add to the list.
5. Be sure to click Apply to save your wireless access control list settings.

Now, only devices on this list will be allowed to wirelessly connect to the WG602 v3. For blocking access from specific devices, follow the procedure above, except select the Block radio button.



Chapter 4
Management

This chapter describes how to use the management features of your 54 Mbps Wireless Access Point WG602 v3. These features can be found under the Management heading in the main menu of the browser interface.

Viewing General Information

The Information summarizes of the current WG602 v3 configuration settings. From the main menu of the browser interface, click Information to view the system status screen, shown below.



Figure 4-1: Wireless Access Point Status screen

This screen shows the following parameters:

Table 4-1. General Information Fields

Field	Description
Access Point Information	
Access Point Name	The default name can be changed if desired.
MAC Address	Displays the Media Access Control address (MAC Addresses) of the wireless access point's Ethernet port.
Region	Displays the country or region for which the wireless access point is licensed for use. It may not be legal to operate this wireless access point in a region other than one of those identified in this field.
Firmware Version	The version of the firmware currently installed.
Current IP Settings	These parameters apply to the Local WG602 v3 wireless access point.
IP Address	The IP address of the wireless access point.
Subnet Mask	The subnet mask for the wireless access point.
Default Gateway	The default gateway for the wireless access point.
DHCP Client	Enabled by default. Enabled (DHCP client) indicates that the current IP address was obtained from a DHCP server on your network.
Wireless Settings	These parameters apply to the target remote WG602 v3, VPN gateway, or VPN client.
Wireless Network Name (SSID)	Displays the wireless network name (SSID) being used by the wireless port of the wireless access point. The default is NETGEAR.
Channel	Identifies the channel the wireless port is using. 11 is the default channel setting. See "Wireless Channels" on page B-2 for the frequencies used on each channel.
Encryption Type	The current encryption setting.
Access Control	Disabled by default.

Viewing a List of Attached Devices

The Station List page contains a table of all IP devices associated with the wireless access point in the wireless network defined by the Wireless Network Name (SSID). From the main menu of the browser interface, under the Management heading, click the Station List link to view the list, shown below.

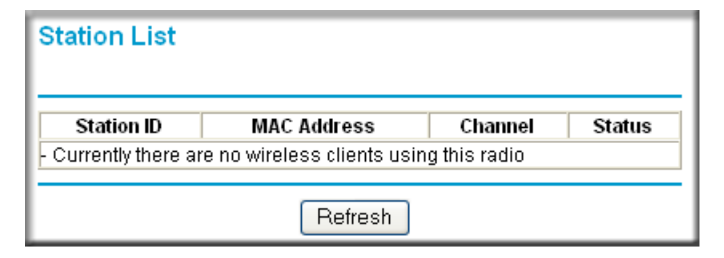


Figure 4-2: Information Station List of associated devices

For each device, the table shows the MAC address and whether the device is allowed to communicate with the wireless access point or not. Note that if the wireless access point is rebooted, the table data is lost until the wireless access point rediscovers the devices. To force the wireless access point to look for associated devices, click the Refresh button.

Note: A wireless network can include multiple wireless access points, all using the same network name (SSID). This enables extending the reach of the wireless network and allows users to roam from one access point to another, providing seamless network connectivity. Under these circumstances, be aware that only the stations associated with this access point will be presented in the Station List.

Upgrading the Wireless Access Point Software



Note: When uploading software to the WG602 v3 Access Point, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, the upload may fail, corrupt the software, and render the WG602 v3 completely inoperable.

You cannot perform the firmware upgrade from a workstation connected to the WG602 v3 via a wireless link. The firmware upgrade must be performed via a workstation connected to the WG602 v3 via the Ethernet LAN interface.

The software of the WG602 v3 Access Point is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR. Upgrade files can be downloaded from the NETGEAR Web site. If the upgrade file is compressed (.ZIP file), you must first extract the image (.IMG) file before sending it to the wireless access point. The upgrade file can be sent using your browser.

Note: The Web browser used to upload new firmware into the WG602 v3 must support HTTP uploads, such as Microsoft Internet Explorer 5.0 or above, or Netscape Navigator 4.78 or above.

1. Download the new software file from NETGEAR, save it to your hard disk, and unzip it.

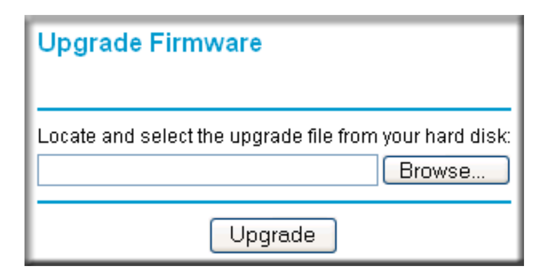


Figure 4-3: WG602 v3 Upgrade Firmware page

2. From the main menu Management section, click the Upgrade Firmware link to display the screen above.
3. Click Browse and locate the image (.IMG) upgrade file.
4. Click Upgrade.

   When the upload completes, your wireless access point will automatically restart. The upgrade process typically takes about one minute.

In some cases, you may need to reconfigure the wireless access point after upgrading. You can click the Information link to check the Firmware Version and verify that your access point now has the new software installed.

Rebooting and Resetting Factory Default Options

The Reboot option restarts the access point. From the Management section of the main menu, select Reboot AP. Select **Yes**, then click **Apply** to reboot the access point.

Restoring the WG602 v3 to the Factory Default Settings

It is sometimes desirable to restore the wireless access point to the factory default settings. This can be done by using the Restore Factory Default function, which restores all factory settings.

After a restore, the password will be **password**, the DHCP client is enabled, the WG602 v3 defaults to the LAN IP address of 192.168.0.227 when there is no DHCP server, and the NetBIOS name is reset to NETGEAR plus the last 6 digits of the MAC address printed on the label on the bottom of the unit, for example *NETGEAR123456*.

On the Restore Factory Default Settings screen, select **Yes**, then click **Apply** to restore the factory default settings.

Using the Reset Button to Reboot or Restore Factory Defaults

To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the wireless access point (see "WG602 v3 Wireless Access Point Rear Panel" on page 2-6). The reset button has two functions:

- **Reboot.** When pressed and released quickly, the wireless access point will reboot (restart).
- **Reset to Factory Defaults.** This button can also be used to clear all data and restore all settings to the factory default values, when held down longer.

To clear all data and restore the factory default values:

1. Use something with a small point, such as a pen, to press the Reset button in for at least 10 seconds.
2. Release the Reset button.

The factory default configuration has now been restored, and the WG602 v3 is ready for use.

Changing the Administrator Password

The default password is **password**. Change this password to a more secure password. You cannot change the administrator login name.

From the main menu of the browser interface, under the Management heading, click Change Password to bring up the page shown below.

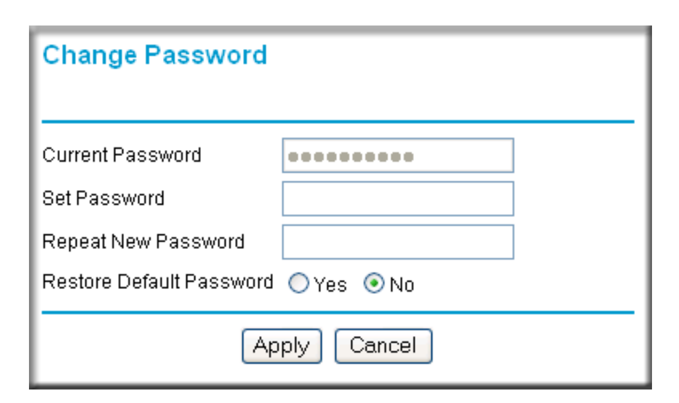


Figure 4-4: Set Password page

To change the password, first enter the old password, and then enter the new password twice. Click Apply to save your change.

Chapter 5
Advanced Configuration

This chapter describes how to configure the advanced features of your WG602 v3. These features can be found under the Advanced heading in the main menu.

Understanding Advanced Wireless Settings

The default advanced wireless settings usually work well. These settings should not be changed unless you are sure it is necessary.

Table 5-1. Advanced Wireless Settings Fields

Field	Description
Request to Send (RTS) Threshold	The packet size that is used to determine whether to use the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) mechanism or the CSMA/CA mechanism for packet transmission. With the CSMA/CD transmission mechanism, the transmitting station sends out the actual packet as soon as it has waited for the silence period. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data.
Fragmentation Length	This is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented. The Fragment Threshold value must be larger than the RTS Threshold value. Default: 2346
Beacon Interval	Specifies the data beacon rate between 20 and 1000.
DTIM Interval	Specifies the Delivery Traffic Indication Message data beacon rate between 1 and 255. Default: 1
Preamble Type	A long transmit preamble may provide a more reliable connection or slightly longer range. A short transmit preamble gives better performance. Default: Mix

Configuring Wireless Distribution System Links

The 54 Mbps Wireless Access Point WG602 v3 lets you build large wireless networks. Examples of wireless bridging configurations are:

- Point-to-point.
- Multi-point.

These features are discussed below.

How to Configure Wireless Bridge Links

To configure wireless bridge links, follow these steps:

1. Click the **Wireless Bridging** link in the Advanced section of the main menu.

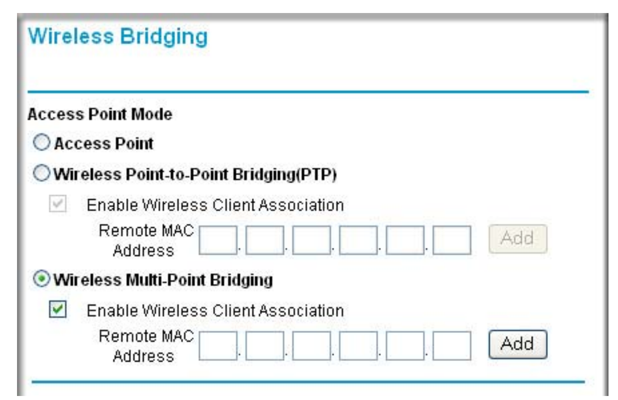


Figure 5-1: Wireless Bridging page

2. Select the radio button for the wireless access point mode you want to configure.
3. Click **Apply** to save your settings.

How to Configure a WG602 v3 as a Point-to-Point Bridge

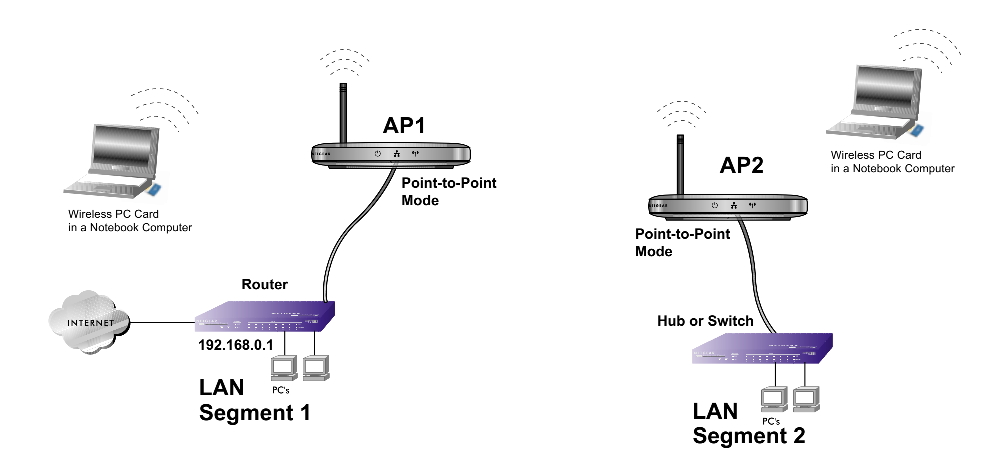


Figure 5-2: Wireless Point-to-Point Bridging

1. Configure AP1 in Point-to-Point mode with the MAC address of AP2 and deploy it on LAN Segment 1. If you check the Enable Wireless Client Association checkbox, wireless clients will also be able to use AP1. If the Enable Wireless Client Association checkbox is not selected, only computers on Ethernet LAN segment 1 will use AP1 to communicate with AP2.
2. Configure AP2 in Point-to-Point mode with the MAC address of AP1 and deploy it on LAN Segment 2. Use the same security and channel settings as AP1. If you check the Enable Wireless Client Association checkbox, wireless clients will also be able to use AP2. If the Enable Wireless Client Association checkbox is not selected, only computers on Ethernet LAN segment 2 will use AP2 to communicate with AP1.
3. Verify connectivity across the network.

   If you enabled wireless client association on both APs, a computer on either AP should be able to connect to the Internet or share files and printers of any other PCs or servers connected to the network.

How to Configure Wireless Multi-Point Bridging

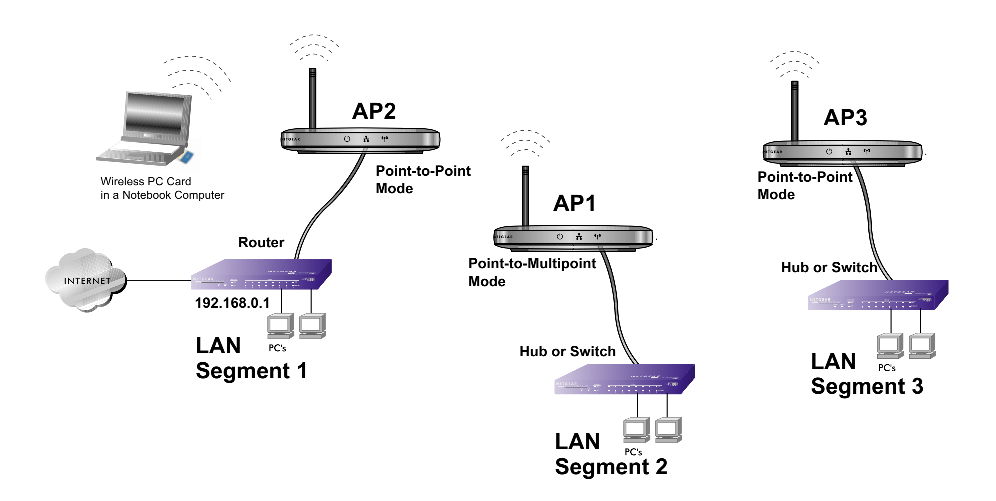


Figure 5-3: Wireless Bridging

1. Configure the Operating Mode of the WG602 v3 Access Points.
   – AP1 on LAN Segment 1 in Point-to-Point Bridge mode with the Remote MAC Address of AP2.
   – Because it is in the central location, configure AP2 on LAN Segment 2 in Wireless Multi-Point Bridging mode. Add the MAC addresses of the adjacent Point-to-Point APs which are configured to communicating with it.
   – Configure the AP3 on LAN 3 in Point-to-Point Bridge mode with the Remote MAC Address of AP2.
2. Verify the following parameters for all access points:
   - Verify that the LAN network configuration the WG602 v3 Access Points are configured to operate in the same LAN network address range as the LAN devices
   - Only one AP is configured in Wireless Multi-Point Bridging mode, and all the others are in Point-to-Point Bridge mode.
   - All APs must be on the same LAN. That is, all the APs LAN IP address must be in the same network.

- If using DHCP, all WG602 v3 Access Points should be set to "Obtain an IP address automatically (DHCP Client)" in the IP Address Source portion of the Basic IP Settings menu.
- All WG602 v3 Access Points use the same SSID, Channel, WEP authentication mode, if any, and encryption in use (WPA is not available in bridge modes).
- All Point-to-Point APs must have AP2's MAC address in its Remote AP MAC address table.
- If MAC access control list security is enabled on the APs, verify that the MAC access control lists on each AP are complete and accurate.

3. Verify connectivity across the LANs.
   - If you check the Enable Wireless Client Association checkbox, wireless clients will also be able to use the AP.
   - A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three LAN segments.
   - If Access Control Lists are enabled on the APs, only computers in the access control list will be able to use the AP.

Note: You can extend this multi-point bridging by adding additional WG602 v3s configured in Point-to-Point mode for additional wireless LAN segments.



Chapter 6
Troubleshooting

This chapter provides information about troubleshooting your 54 Mbps Wireless Access Point WG602 v3. After each problem description, instructions are given to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the WG602 v3 on?
- Have I connected the wireless access point correctly?

  Go to "Installing the 54 Mbps Wireless Access Point WG602 v3" on page 3-4.
- I cannot remember the wireless access point's configuration password.

  Go to "Changing the Administrator Password" on page 4-6.



Note: For up-to-date WG602 v3 installation details and troubleshooting guidance visit *http://kbserver.netgear.com/products/WG602v3.asp*.

Troubleshooting

If you have trouble setting up your WG602 v3, check the tips below.

No lights are lit on the access point.

The access point has no power.

- Make sure the power cord is connected to the access point and plugged in to a working power outlet or power strip.
- Make sure you are using the correct NETGEAR power adapter supplied with your access point.

The Ethernet LAN light is not lit.

There is a hardware connection problem.

- Make sure the cable connectors are securely plugged in at the access point and the network device (hub, switch, or router).
- Make sure the connected device is turned on.
- Be sure the correct cable is used. Use a standard Category 5 Ethernet patch cable. If the network device has Auto Uplink™ (MDI/MDIX) ports, you may use a cross-over cable. See the Reference Manual for a full explanation of cable types.

The Wireless LAN activity light is not lit.

The access point's antenna is not working.

- If the Wireless LAN activity light stays off, disconnect the adapter from its power source and then plug it in again.
- Make sure the antenna is tightly connected to the WG602 v3.
- Contact NETGEAR if the Wireless LAN light remains off.

I cannot configure the wireless access point from a browser.

Check these items:

- The WG602 v3 is properly installed, LAN connections are OK, and it is powered on. Check that the LAN port LED is amber or green to verify that the Ethernet connection is OK.
- If you are using the NetBIOS name of the WG602 v3 to connect, ensure that your PC and the WG602 v3 are on the same network segment or that there is a WINS server on your network.
- If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address in the range of the WG602 v3. The WG602 v3 default IP Address is 192.168.0.227 and the default Subnet Mask is 255.255.255.0. If you are not sure about these settings, follow the instructions for "Installing the 54 Mbps Wireless Access Point WG602 v3" on page 3-4.

I cannot access the Internet or the LAN with a wireless capable computer.

There is a configuration problem. Check these items:

- You may not have restarted the computer with the wireless adapter to have TCP/IP changes take effect. Restart the computer.

- The computer with the wireless adapter may not have the correct TCP/IP settings to communicate with the network. Restart the computer and check that TCP/IP is set up properly for that network. The usual setting for Windows Network Properties is "Obtain an IP address automatically."
- The access point's default values may not work with your network. Check the access point default configuration against the configuration of other devices in your network.
- For full instructions on changing the access point's default values, see the Reference Manual on the *Resource CD for the 54 Mbps Wireless Access Point WG602 v3 (230-10106-01)*.

When I enter a URL or IP address I get a timeout error.

A number of things could be causing this. Try the following troubleshooting steps:

- Check whether other PCs work. If they do, ensure that your PCs TCP/IP settings are correct. If using a Fixed (Static) IP Address, check the Subnet Mask, Default Gateway, DNS, and IP Addresses.
- If the PCs are configured correctly, but still not working, ensure that the WG602 v3 is connected and turned on. Connect to it and check its settings. If you cannot connect to it, check the LAN and power connections.
- If the WG602 v3 is configured correctly, check your Internet connection (DSL/Cable modem etc.) to make sure that it is working correctly.

Using the Reset Button to Restore Factory Default Settings

The Reset button (see "WG602 v3 Wireless Access Point Rear Panel" on page 2-6) has two functions:

- **Reboot.** When pressed and released quickly, the WG602 v3 will reboot (restart).
- **Reset to Factory Defaults.** This button can also be used to clear ALL data and restore ALL settings to the factory default values.

To clear all data and restore the factory default values:

1. Use something with a small point, such as a pen, to press the Reset button in for at least 10 seconds.
2. Release the Reset button.

The factory default configuration has now been restored, and the WG602 v3 is ready for use.

Appendix A
Specifications

This appendix provides the 54 Mbps Wireless Access Point WG602 v3 technical specifications.

Specifications for the WG602 v3

Parameter	54 Mbps Wireless Access Point WG602 v3
Radio Data Rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps Auto Rate Sensing
Frequency	2.4-2.5Ghz
Data Encoding:	Direct Sequence Spread Spectrum (DSSS) for 802.11b and Orthogonal Frequency Division Multiplexing (OFDM) for 802.11g
Wireless Security:	WEP and WPA-PSK
Maximum Computers Per Wireless Network:	Limited by the amount of wireless network traffic generated by each node. Typically 32 nodes.
Network Management	Web-based configuration and status monitoring
Status LEDs	Power/Ethernet LAN/Wireless LAN
Dimensions:	28 x 175 x 118 mm (1.1 x 6.89 x 4.65 in.)
Power Adapter	7.5Vdc, 1A
Weight	845 g (29.7 oz)
Electromagnetic Compliance	FCC Part 15 Class B and Class E, CE, C-tic AS/NZS 3548, Telec STD-T66, VCCI
Environmental Specifications	Operating temperature: 0 to 50° C Operating humidity: 5-95%, non-condensing

Appendix B
Wireless Networking Basics

This chapter provides an overview of wireless networking and security.

Wireless Networking Overview

The WG602 v3 Access Point conforms to the Institute of Electrical and Electronics Engineers (IEEE) 802.11g standard for wireless LANs (WLANs). On an 802.11 wireless link, data is encoded using direct-sequence spread-spectrum (DSSS) technology and is transmitted in the unlicensed radio spectrum at 2.5GHz. The maximum data rate for the 802.11g wireless link is 54 Mbps, but it will automatically back down from 54 Mbps when the radio signal is weak or when interference is detected.

The 802.11 standard is also called Wireless Ethernet or Wi-Fi by the Wireless Ethernet Compatibility Alliance (WECA, see *http://www.wi-fi.net*), an industry standard group promoting interoperability among 802.11 devices. The 802.11 standard offers two methods for configuring a wireless network - ad hoc and infrastructure.

Infrastructure Mode

With a wireless access point, you can operate the wireless LAN in the infrastructure mode. This mode provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage, interacting with wireless nodes via an antenna.

In the infrastructure mode, the wireless access point converts airwave data into wired Ethernet data, acting as a bridge between the wired LAN and wireless clients. Connecting multiple access points via a wired Ethernet backbone can further extend the wireless network coverage. As a mobile computing device moves out of the range of one access point, it moves into the range of another. As a result, wireless clients can freely roam from one access point domain to another and still maintain seamless network connection.

Ad Hoc Mode (Peer-to-Peer Workgroup)

In an ad hoc network, computers are brought together as needed; thus, there is no structure or fixed points to the network - each node can generally communicate with any other node. There is no access point involved in this configuration. This mode enables you to quickly set up a small wireless workgroup and allows workgroup members to exchange data or share printers as supported by Microsoft networking in the various Windows operating systems. Some vendors also refer to ad hoc networking as peer-to-peer group networking.

In this configuration, network packets are directly sent and received by the intended transmitting and receiving stations. As long as the stations are within range of one another, this is the easiest and least expensive way to set up a wireless network.

Network Name: Extended Service Set Identification (ESSID)

The Extended Service Set Identification (ESSID) is one of two types of Service Set Identification (SSID). In an ad hoc wireless network with no access points, the Basic Service Set Identification (BSSID) is used. In an infrastructure wireless network that includes an access point, the ESSID is used, but may still be referred to as SSID.

An SSID is a thirty-two character (maximum) alphanumeric key identifying the name of the wireless local area network. Some vendors refer to the SSID as network name. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID.

Wireless Channels

IEEE 802.11g/b wireless nodes communicate with each other using radio frequency signals in the ISM (Industrial, Scientific, and Medical) band between 2.4 GHz and 2.5 GHz. Neighboring channels are 5 MHz apart. However, due to spread spectrum effect of the signals, a node sending signals using a particular channel will utilize frequency spectrum 12.5 MHz above and below the center channel frequency. As a result, two separate wireless networks using neighboring channels (for example, channel 1 and channel 2) in the same general vicinity will interfere with each other. Applying two channels that allow the maximum channel separation will decrease the amount of channel cross-talk, and provide a noticeable performance increase over networks with minimal channel separation.

The radio frequency channels used are listed in Table B-1:

Table B-1. 802.11b Radio Frequency Channels

Channel	Center Frequency	Frequency Spread
1	2412 MHz	2399.5 MHz - 2424.5 MHz
2	2417 MHz	2404.5 MHz - 2429.5 MHz
3	2422 MHz	2409.5 MHz - 2434.5 MHz
4	2427 MHz	2414.5 MHz - 2439.5 MHz
5	2432 MHz	2419.5 MHz - 2444.5 MHz
6	2437 MHz	2424.5 MHz - 2449.5 MHz
7	2442 MHz	2429.5 MHz - 2454.5 MHz
8	2447 MHz	2434.5 MHz - 2459.5 MHz
9	2452 MHz	2439.5 MHz - 2464.5 MHz
10	2457 MHz	2444.5 MHz - 2469.5 MHz
11	2462 MHz	2449.5 MHz - 2474.5 MHz
12	2467 MHz	2454.5 MHz - 2479.5 MHz
13	2472 MHz	2459.5 MHz - 2484.5 MHz

Note: The available channels supported by the wireless products in various countries are different.

The preferred channel separation between the channels in neighboring wireless networks is 25 MHz (5 channels). This means that you can apply up to three different channels within your wireless network. There are only 11 usable wireless channels in the United States. It is recommended that you start using channel 1 and grow to use channel 6, and 11 when necessary, as these three channels do not overlap.

WEP Wireless Security

The absence of a physical connection between nodes makes the wireless links vulnerable to eavesdropping and information theft. To provide a certain level of security, the IEEE 802.11 standard has defined two types of authentication methods, Open System and Shared Key. With Open System authentication, a wireless PC can join any network and receive any messages that are not encrypted. With Shared Key authentication, only those PCs that possess the correct authentication key can join the network. By default, IEEE 802.11 wireless devices operate in an Open System network. Recently, Wi-Fi, the Wireless Ethernet Compatibility Alliance (*http://www.wi-fi.net*) developed the Wi-Fi Protected Access (WPA), a new strongly enhanced Wi-Fi security. WPA will soon be incorporated into the IEEE 802.11 standard. WEP and WPA are discussed below.

WEP Authentication

The 802.11 standard defines several services that govern how two 802.11 devices communicate. The following events must occur before an 802.11 Station can communicate with an Ethernet network through an access point such as the one built in to the WG602 v3:

1. Turn on the wireless station.
2. The station listens for messages from any access points that are in range.
3. The station finds a message from an access point that has a matching SSID.
4. The station sends an authentication request to the access point.
5. The access point authenticates the station.
6. The station sends an association request to the access point.
7. The access point associates with the station.
8. The station can now communicate with the Ethernet network through the access point.

An access point must authenticate a station before the station can associate with the access point or communicate with the network. The IEEE 802.11 standard defines two types of WEP authentication: Open System and Shared Key.

- Open System Authentication allows any device to join the network, assuming that the device SSID matches the access point SSID. Alternatively, the device can use the “ANY” SSID option to associate with any available access point within range, regardless of its SSID.

- Shared Key Authentication requires that the station and the access point have the same WEP Key to authenticate. These two authentication procedures are described below.

WEP Open System Authentication

This process is illustrated in below.

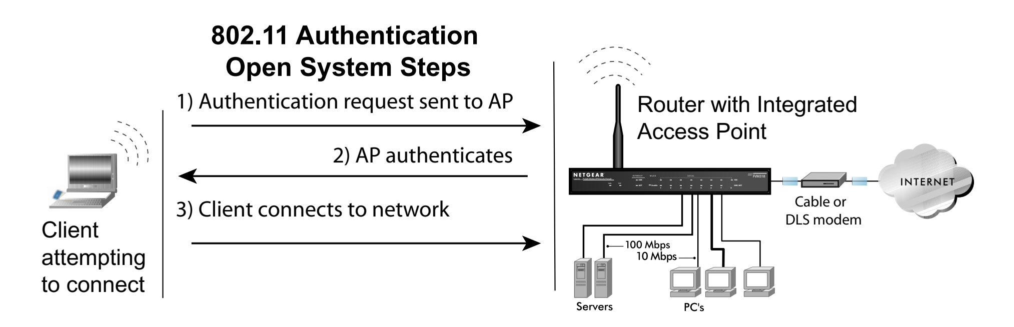


Figure B-1: 802.11 open system authentication

The following steps occur when two devices use Open System Authentication:

1. The station sends an authentication request to the access point.
2. The access point authenticates the station.
3. The station associates with the access point and joins the network.

WEP Shared Key Authentication

This process is illustrated in below.

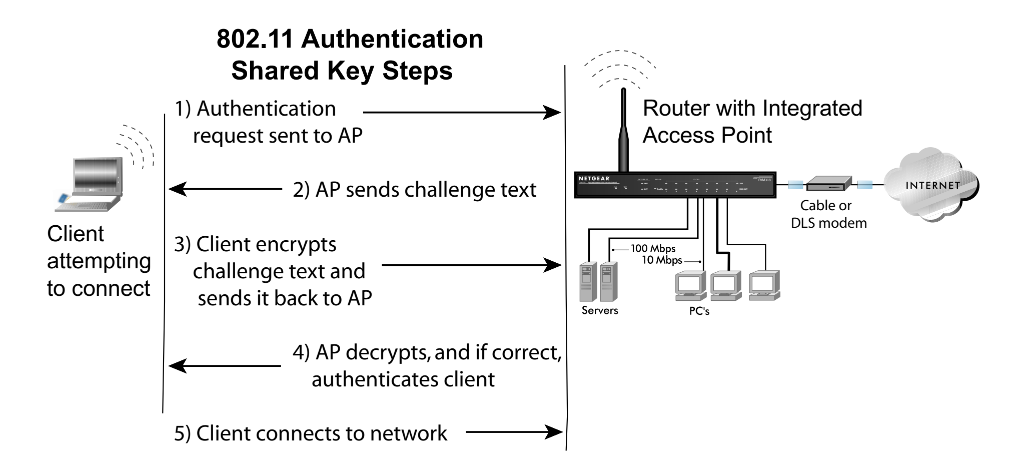


Figure B-2: 802.11 shared key authentication

The following steps occur when two devices use Shared Key Authentication:

1. The station sends an authentication request to the access point.
2. The access point sends challenge text to the station.
3. The station uses its configured 64-bit or 128-bit default key to encrypt the challenge text, and sends the encrypted text to the access point.
4. The access point decrypts the encrypted text using its configured WEP Key that corresponds to the station's default key. The access point compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, then the access point and the station share the same WEP Key and the access point authenticates the station.
5. The station connects to the network.

If the decrypted text does not match the original challenge text (i.e., the access point and station do not share the same WEP Key), then the access point will refuse to authenticate the station and the station will be unable to communicate with either the 802.11 network or Ethernet network.

Key Size and Configuration

The IEEE 802.11 standard supports two types of WEP encryption: 40-bit and 128-bit.

The 64-bit WEP data encryption method, allows for a five-character (40-bit) input. Additionally, 24 factory-set bits are added to the forty-bit input to generate a 64-bit encryption key. (The 24 factory-set bits are not user-configurable). This encryption key will be used to encrypt/decrypt all data transmitted via the wireless interface. Some vendors refer to the 64-bit WEP data encryption as 40-bit WEP data encryption since the user-configurable portion of the encryption key is 40 bits wide.

The 128-bit WEP data encryption method consists of 104 user-configurable bits. Similar to the forty-bit WEP data encryption method, the remaining 24 bits are factory set and not user configurable. Some vendors allow passphrases to be entered instead of the cryptic hexadecimal characters to ease encryption key entry.

128-bit encryption is stronger than 40-bit encryption, but 128-bit encryption may not be available outside of the United States due to U.S. export regulations.

When configured for 40-bit encryption, 802.11 products typically support up to four WEP Keys. Each 40-bit WEP Key is expressed as 5 sets of two hexadecimal digits (0-9 and A-F). For example, “12 34 56 78 90” is a 40-bit WEP Key.

When configured for 128-bit encryption, 802.11b products typically support four WEP Keys but some manufacturers support only one 128-bit key. The 128-bit WEP Key is expressed as 13 sets of two hexadecimal digits (0-9 and A-F). For example, “12 34 56 78 90 AB CD EF 12 34 56 78 90” is a 128-bit WEP Key.

Typically, 802.11 access points can store up to four 128-bit WEP Keys but some 802.11 client adapters can only store one. Therefore, make sure that your 802.11 access and client adapters configurations match.

Whatever keys you enter for an AP, you must also enter the same keys for the client adapter in the same order. In other words, WEP key 1 on the AP must match WEP key 1 on the client adapter, WEP key 2 on the AP must match WEP key 2 on the client adapter, etc.

Note: The AP and the client adapters can have different default WEP Keys as long as the keys are in the same order. In other words, the AP can use WEP key 2 as its default key to transmit while a client adapter can use WEP key 3 as its default key to transmit. The two devices will communicate as long as the AP's WEP key 2 is the same as the client's WEP key 2 and the AP's WEP key 3 is the same as the client's WEP key 3.

How to Use WEP Parameters

Wired Equivalent Privacy (WEP) data encryption is used when the wireless devices are configured to operate in Shared Key authentication mode. There are two shared key methods implemented in most commercially available products, 64-bit and 128-bit WEP data encryption.

Before enabling WEP on an 802.11 network, you must first consider what type of encryption you require and the key size you want to use. Typically, there are three WEP Encryption options available for 802.11 products:

1. **Do Not Use WEP:** The 802.11 network does not encrypt data. For authentication purposes, the network uses Open System Authentication.

2. **Use WEP for Encryption:** A transmitting 802.11 device encrypts the data portion of every packet it sends using a configured WEP Key. The receiving 802.11b device decrypts the data using the same WEP Key. For authentication purposes, the 802.11b network uses Open System Authentication.

3. **Use WEP for Authentication and Encryption:** A transmitting 802.11 device encrypts the data portion of every packet it sends using a configured WEP Key. The receiving 802.11 device decrypts the data using the same WEP Key. For authentication purposes, the 802.11 network uses Shared Key Authentication.

Note: Some 802.11 access points also support **Use WEP for Authentication Only** (Shared Key Authentication without data encryption). However, the WG602 v3 does not offer this option.

WPA Wireless Security

Wi-Fi Protected Access (WPA) is a specification of standards-based, interoperable security enhancements that increase the level of data protection and access control for existing and future wireless LAN systems.

The IEEE introduced the WEP as an optional security measure to secure 802.11b (Wi-Fi) WLANs, but inherent weaknesses in the standard soon became obvious. In response to this situation, the Wi-Fi Alliance announced a new security architecture in October 2002 that remedies the short comings of WEP. This standard, formerly known as Safe Secure Network (SSN), is designed to work with existing 802.11 products and offers forward compatibility with 802.11i, the new wireless security architecture being defined in the IEEE.

WPA offers the following benefits:

- Enhanced data privacy
- Robust key management
- Data origin authentication
- Data integrity protection

The Wi-Fi Alliance is now performing interoperability certification testing on Wi-Fi Protected Access products. Starting August of 2003, all new Wi-Fi certified products will have to support WPA. NETGEAR will implement WPA on client and access point products and make this available in the second half of 2003. Existing Wi-Fi certified products will have one year to add WPA support or they will loose their Wi-Fi certification.

The 802.11i standard is currently in draft form, with ratification due at the end of 2003. While the new IEEE 802.11i standard is being ratified, wireless vendors have agreed on WPA as an interoperable interim standard.

How Does WPA Compare to WEP?

WEP is a data encryption method and is not intended as a user authentication mechanism. WPA user authentication is implemented using 802.1x and the Extensible Authentication Protocol (EAP). Support for 802.1x authentication is required in WPA. In the 802.11 standard, 802.1x authentication was optional. For details on EAP specifically, refer to IETF's RFC 2284.

With 802.11 WEP, all access points and client wireless adapters on a particular wireless LAN must use the same encryption key. A major problem with the 802.11 standard is that the keys are cumbersome to change. If you don't update the WEP keys often, an unauthorized person with a sniffing tool can monitor your network for less than a day and decode the encrypted messages. Products based on the 802.11 standard alone offer system administrators no effective method to update the keys.

For 802.11, WEP encryption is optional. For WPA, encryption using Temporal Key Integrity Protocol (TKIP) is required. TKIP replaces WEP with a new encryption algorithm that is stronger than the WEP algorithm, but that uses the calculation facilities present on existing wireless devices to perform encryption operations. TKIP provides important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. Through these enhancements, TKIP addresses all of known WEP vulnerabilities.

How Does WPA Compare to IEEE 802.11i?

WPA will be forward compatible with the IEEE 802.11i security specification currently under development. WPA is a subset of the current 802.11i draft and uses certain pieces of the 802.11i draft that are ready to bring to market today, such as 802.1x and TKIP. The main pieces of the 802.11i draft that are not included in WPA are secure IBSS (Ad-Hoc mode), secure fast handoff (for specialized 802.11 VoIP phones), as well as enhanced encryption protocols such as AES-CCMP. These features are either not yet ready for market or will require hardware upgrades to implement.

What are the Key Features of WPA Security?

The following security features are included in the WPA standard:

- WPA Authentication
- WPA Encryption Key Management
  - Temporal Key Integrity Protocol (TKIP)
  - Michael *message integrity code* (MIC)
  - AES Support
- Support for a Mixture of WPA and WEP Wireless Clients

These features are discussed below.

WPA addresses most of the known WEP vulnerabilities and is primarily intended for wireless infrastructure networks as found in the enterprise. This infrastructure includes stations, access points, and authentication servers (typically RADIUS servers). The RADIUS server holds (or has access to) user credentials (e.g., user names and passwords) and authenticates wireless users before they gain access to the network.

The strength WPA comes from an integrated sequence of operations that encompass 802.1X/EAP authentication and sophisticated key management and encryption techniques. Its major operations include:

- Network security capability determination. This occurs at the 802.11 level and is communicated through WPA information elements in Beacon, Probe Response, and (Re) Association Requests. Information in these elements includes the authentication method (802.1X or Pre-shared key) and the preferred cipher suite (WEP, TKIP, or AES).

The primary information conveyed in the Beacon frames is the authentication method and the cipher suite. Possible authentication methods include 802.1X and Pre-shared key. Pre-shared key is an authentication method that uses a statically configured pass phrase on both the stations and the access point. This obviates the need for an authentication server, which in many home and small office environments will not be available nor desirable. Possible cipher suites include: WEP, TKIP, and AES (Advanced Encryption Standard). We'll talk more TKIP and AES when addressing data privacy below.

- Authentication. EAP over 802.1X is used for authentication. Mutual authentication is gained by choosing an EAP type supporting this feature and is required by WPA. 802.1X port access control prevents full access to the network until authentication completes. 802.1X EAPOL-Key packets are used by WPA to distribute per-session keys to those stations successfully authenticated.

  The supplicant in the station uses the authentication and cipher suite information contained in the information elements to decide which authentication method and cipher suite to use. For example, if the access point is using the Pre-shared key method then the supplicant need not authenticate using full-blown 802.1X. Rather, the supplicant must simply prove to the access point that it is in possession of the pre-shared key. If the supplicant detects that the service set does not contain a WPA information element then it knows it must use pre-WPA 802.1X authentication and key management in order to access the network.

- Key management. WPA features a robust key generation/management system that integrates the authentication and data privacy functions. Keys are generated after successful authentication and through a subsequent 4-way handshake between the station and Access Point (AP).
- Data Privacy (Encryption). Temporal Key Integrity Protocol (TKIP) is used to wrap WEP in sophisticated cryptographic and security techniques to overcome most of its weaknesses.
- Data integrity. TKIP includes a message integrity code (MIC) at the end of each plaintext message to ensure messages are not being spoofed.

WPA Authentication: Enterprise-level User Authentication via 802.1x/EAP and RADIUS

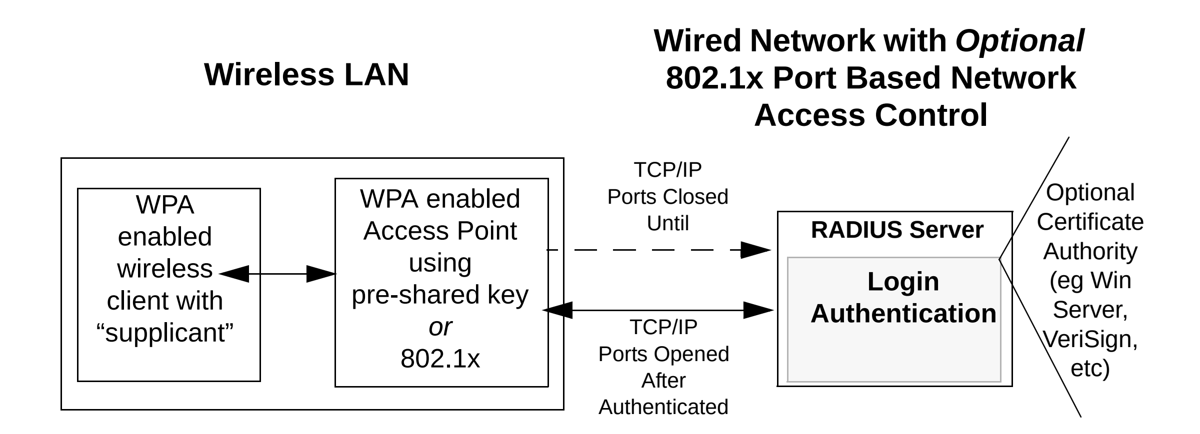


Figure B-3: WPA Overview

IEEE 802.1x offers an effective framework for authenticating and controlling user traffic to a protected network, as well as providing a vehicle for dynamically varying data encryption keys via EAP from a RADIUS server, for example. This framework enables using a central authentication server, which employs mutual authentication so that a rogue wireless user does not join the network.

It's important to note that 802.1x doesn't provide the actual authentication mechanisms. When using 802.1x, the EAP type, such as Transport Layer Security (EAP-TLS) or EAP Tunneled Transport Layer Security (EAP-TTLS) defines how the authentication takes place.

Note: For environments with a Remote Authentication Dial-In User Service (RADIUS) infrastructure, WPA supports Extensible Authentication Protocol (EAP). For environments without a RADIUS infrastructure, WPA supports the use of a preshared key.

Together, these technologies provide a framework for strong user authentication.

Windows XP implements 802.1x natively, and several Netgear switch and wireless access point products support 802.1x.

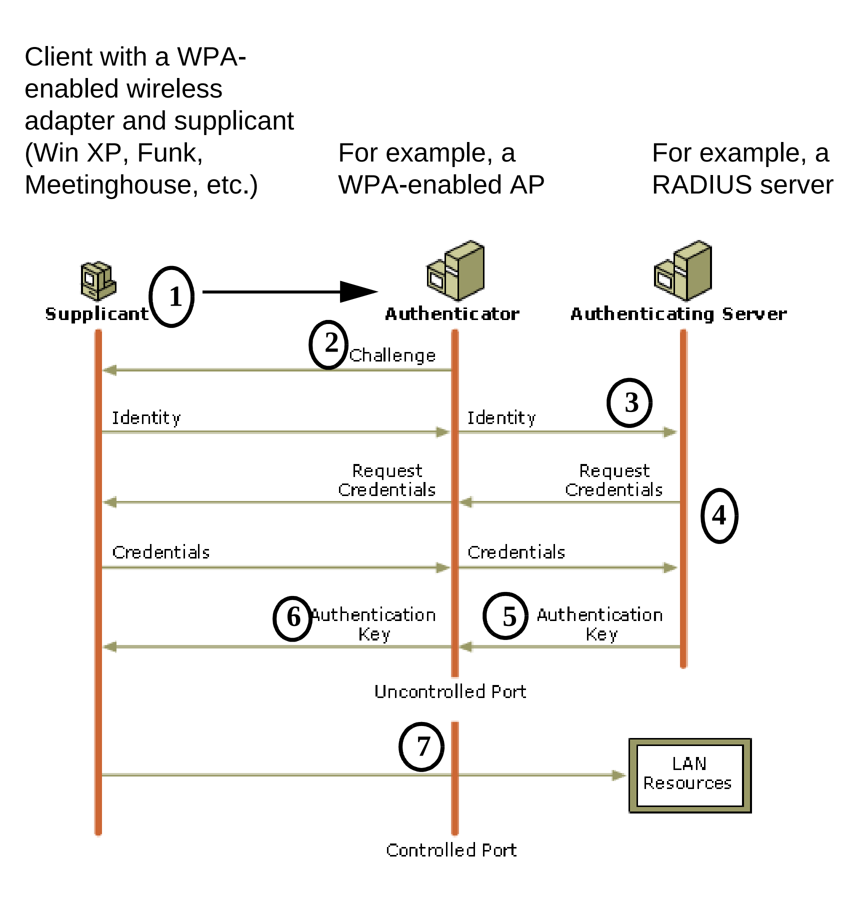


Figure B-4: 802.1x Authentication Sequence

The AP sends Beacon Frames with WPA information element to the stations in the service set. Information elements include the required authentication method (802.1x or Pre-shared key) and the preferred cipher suite (WEP, TKIP, or AES). Probe Responses (AP to station) and Association Requests (station to AP) also contain WPA information elements.

1. Initial 802.1x communications begin with an unauthenticated supplicant (i.e., client device) attempting to connect with an authenticator (i.e., 802.11 access point). The client sends an EAP-start message. This begins a series of message exchanges to authenticate the client.
2. The access point replies with an EAP-request identity message.

3. The client sends an EAP-response packet containing the identity to the authentication server. The access point responds by enabling a port for passing only EAP packets from the client to an authentication server located on the wired side of the access point. The access point blocks all other traffic, such as HTTP, DHCP, and POP3 packets, until the access point can verify the client's identity using an authentication server (e.g., RADIUS).
4. The authentication server uses a specific authentication algorithm to verify the client's identity. This could be through the use of digital certificates or some other EAP authentication type.
5. The authentication server will either send an accept or reject message to the access point.
6. The access point sends an EAP-success packet (or reject packet) to the client.
7. If the authentication server accepts the client, then the access point will transition the client's port to an authorized state and forward additional traffic.

The important part to know at this point is that the software supporting the specific EAP type resides on the authentication server and within the operating system or application “supplicant” software on the client devices. The access point acts as a “pass through” for 802.1x messages, which means that you can specify any EAP type without needing to upgrade an 802.1x-compliant access point. As a result, you can update the EAP authentication type to such devices as token cards (Smart Cards), Kerberos, one-time passwords, certificates, and public key authentication or as newer types become available and your requirements for security change.

WPA Data Encryption Key Management

With 802.1x, the rekeying of unicast encryption keys is optional. Additionally, 802.11 and 802.1x provide no mechanism to change the global encryption key used for multicast and broadcast traffic. With WPA, rekeying of both unicast and global encryption keys is required.

For the unicast encryption key, the Temporal Key Integrity Protocol (TKIP) changes the key for every frame, and the change is synchronized between the wireless client and the wireless access point (AP). For the global encryption key, WPA includes a facility (the Information Element) for the wireless AP to advertise the changed key to the connected wireless clients.

If configured to implement dynamic key exchange, the 802.1x authentication server can return session keys to the access point along with the accept message. The access point uses the session keys to build, sign and encrypt an EAP key message that is sent to the client immediately after sending the success message. The client can then use contents of the key message to define applicable encryption keys. In typical 802.1x implementations, the client can automatically change encryption keys as often as necessary to minimize the possibility of eavesdroppers having enough time to crack the key in current use.

Temporal Key Integrity Protocol (TKIP)

WPA uses TKIP to provide important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. TKIP also provides for the following:

- The verification of the security configuration after the encryption keys are determined.
- The synchronized changing of the unicast encryption key for each frame.
- The determination of a unique starting unicast encryption key for each preshared key authentication.

Michael

With 802.11 and WEP, data integrity is provided by a 32-bit *integrity check value* (ICV) that is appended to the 802.11 payload and encrypted with WEP. Although the ICV is encrypted, you can use cryptanalysis to change bits in the encrypted payload and update the encrypted ICV without being detected by the receiver.

With WPA, a method known as *Michael* specifies a new algorithm that calculates an 8-byte *message integrity code* (MIC) using the calculation facilities available on existing wireless devices. The MIC is placed between the data portion of the IEEE 802.11 frame and the 4-byte ICV. The MIC field is encrypted together with the frame data and the ICV.

Michael also provides replay protection. A new frame counter in the IEEE 802.11 frame is used to prevent replay attacks.

AES Support

One of the encryption methods supported by WPA beside TKIP is the advanced encryption standard (AES), although AES support will not be required initially for Wi-Fi certification. This is viewed as the optimal choice for security conscience organizations, but the problem with AES is that it requires a fundamental redesign of the NIC's hardware in both the station and the access point. TKIP was a pragmatic compromise that allows organizations to deploy better security while AES capable equipment is being designed, manufactured, and incrementally deployed.

Is WPA Perfect?

WPA is not without its vulnerabilities. Specifically, it is susceptible to denial of service (DoS) attacks. If the access point receives two data packets that fail the Message Integrity Code (MIC) check within 60 seconds of each other then the network is under an active attack, and as a result, the access point employs counter measures, which includes disassociating each station using the access point. This prevents an attacker from gleaning information about the encryption key and alerts administrators, but it also causes users to lose network connectivity for 60 seconds. More than anything else, this may just prove that no single security tactic is completely invulnerable. WPA is a definite step forward in WLAN security over WEP and has to be thought of as a single part of an end-to-end network security strategy.

Product Support for WPA

Starting in August, 2003, NETGEAR, Inc. wireless Wi-Fi certified products will support the WPA standard. NETGEAR, Inc. wireless products that had their Wi-Fi certification approved before August, 2003 will have one year to add WPA so as to maintain their Wi-Fi certification.

WPA requires software changes to the following:

- Wireless access points
- Wireless network adapters
- Wireless client programs

Supporting a Mixture of WPA and WEP Wireless Clients

To support the gradual transition of WEP-based wireless networks to WPA, a wireless AP can support both WEP and WPA clients at the same time. During the association, the wireless AP determines which clients use WEP and which clients use WPA. The disadvantage to supporting a mixture of WEP and WPA clients is that the global encryption key is not dynamic. This is because WEP-based clients cannot support it. All other benefits to the WPA clients, such as integrity, are maintained.

However, a mixed mode supporting WPA and non-WPA clients would offer network security that is no better than that obtained with a non-WPA network, and thus this mode of operation is discouraged.

Changes to Wireless Access Points

Wireless access points must have their firmware updated to support the following:

- **The new WPA information element**
  To advertise their support of WPA, wireless APs send the beacon frame with a new 802.11 WPA information element that contains the wireless AP's security configuration (encryption algorithms and wireless security configuration information).
- **The WPA two-phase authentication**
  Open system, then 802.1x (EAP with RADIUS or preshared key).
- **TKIP**
- **Michael**
- **AES** (optional)

To upgrade your wireless access points to support WPA, obtain a WPA firmware update from your wireless AP vendor and upload it to your wireless AP.

Changes to Wireless Network Adapters

Wireless network adapters must have their firmware updated to support the following:

- **The new WPA information element**
  Wireless clients must be able to process the WPA information element and respond with a specific security configuration.
- **The WPA two-phase authentication**
  Open system, then 802.1x (EAP or preshared key).
- **TKIP**
- **Michael**
- **AES** (optional)

To upgrade your wireless network adapters to support WPA, obtain a WPA update from your wireless network adapter vendor and update the wireless network adapter driver.

For Windows wireless clients, you must obtain an updated network adapter driver that supports WPA. For wireless network adapter drivers that are compatible with Windows XP (Service Pack 1) and Windows Server 2003, the updated network adapter driver must be able to pass the adapter's WPA capabilities and security configuration to the Wireless Zero Configuration service.

Microsoft has worked with many wireless vendors to embed the WPA firmware update in the wireless adapter driver. So, to update you Windows wireless client, all you have to do is obtain the new WPA-compatible driver and install the driver. The firmware is automatically updated when the wireless network adapter driver is loaded in Windows.

Changes to Wireless Client Programs

Wireless client programs must be updated to permit the configuration of WPA authentication (and preshared key) and the new WPA encryption algorithms (TKIP and the optional AES component).

To obtain the Microsoft WPA client program, visit the following Microsoft Web site.

Appendix C
Network, Routing, Firewall, and Cabling Basics

This chapter provides an overview of IP networks, routing, and wireless networking.

As you read this document, you may be directed to various RFC documents for further information. An RFC is a Request For Comment (RFC) published by the Internet Engineering Task Force (IETF), an open organization that defines the architecture and operation of the Internet. The RFC documents outline and define the standard protocols and procedures for the Internet. The documents are listed on the World Wide Web at *www.ietf.org* and are mirrored and indexed at many other sites worldwide.

Basic Router Concepts

Large amounts of bandwidth can be provided easily and relatively inexpensively in a local area network (LAN). However, providing high bandwidth between a local network and the Internet can be very expensive. Because of this expense, Internet access is usually provided by a slower-speed wide-area network (WAN) link such as a cable or DSL modem. In order to make the best use of the slower WAN link, a mechanism must be in place for selecting and transmitting only the data traffic meant for the Internet. The function of selecting and forwarding this data is performed by a router.

What is a Router?

A router is a device that forwards traffic between networks based on network layer information in the data and on routing tables maintained by the router. In these routing tables, a router builds up a logical picture of the overall network by gathering and exchanging information with other routers in the network. Using this information, the router chooses the best path for forwarding network traffic.

Routers vary in performance and scale, number of routing protocols supported, and types of physical WAN connection they support. The 54 Mbps Wireless Access Point WG602 v3 is a small office router that routes the IP protocol over a single-user broadband connection.

IP Addresses and the Internet

Because TCP/IP networks are interconnected across the world, every machine on the Internet must have a unique address to make sure that transmitted data reaches the correct destination. Blocks of addresses are assigned to organizations by the Internet Assigned Numbers Authority (IANA). Individual users and small organizations may obtain their addresses either from the IANA or from an Internet service provider (ISP). You can contact IANA at www.iana.org.

The Internet Protocol (IP) uses a 32-bit address structure. The address is usually written in dot notation (also called dotted-decimal notation), in which each group of eight bits is written in decimal form, separated by decimal points.

For example, the following binary address: 11000011 00100010 00001100 00000111

is normally written as: 195.34.12.7

The latter version is easier to remember and easier to enter into your computer.

In addition, the 32 bits of the address are subdivided into two parts. The first part of the address identifies the network, and the second part identifies the host node or station on the network. The dividing point may vary depending on the address range and the application.

There are five standard classes of IP addresses. These address classes have different ways of determining the network and host sections of the address, allowing for different numbers of hosts on a network. Each address type begins with a unique bit pattern, which is used by the TCP/IP software to identify the address class. After the address class has been determined, the software can correctly identify the host section of the address. The follow figure shows the three main address classes, including network and host sections of the address for each address type.

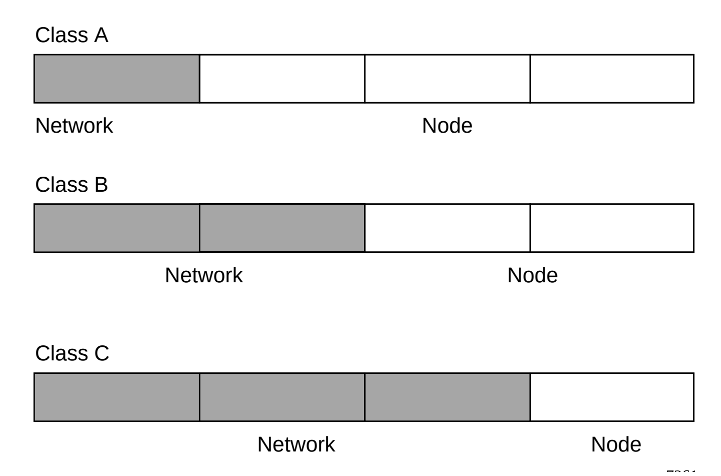


Figure C-1: Three Main Address Classes

The five address classes are:

- Class A
  Class A addresses can have up to 16,777,214 hosts on a single network. They use an eight-bit network number and a 24-bit node number. Class A addresses are in this range:

  `1.x.x.x to 126.x.x.x.`

- Class B
  Class B addresses can have up to 65,354 hosts on a network. A Class B address uses a 16-bit network number and a 16-bit node number. Class B addresses are in this range:

  `128.1.x.x to 191.254.x.x.`

- Class C
  Class C addresses can have 254 hosts on a network. Class C addresses use 24 bits for the network address and eight bits for the node. They are in this range:

  `192.0.1.x to 223.255.254.x.`

- Class D
  Class D addresses are used for multicasts (messages sent to many hosts). Class D addresses are in this range:

  `224.0.0.0 to 239.255.255.255.`

- Class E
  Class E addresses are for experimental use.

This addressing structure allows IP addresses to uniquely identify each physical network and each node on each physical network.

For each unique value of the network portion of the address, the base address of the range (host address of all zeros) is known as the network address and is not usually assigned to a host. Also, the top address of the range (host address of all ones) is not assigned, but is used as the broadcast address for simultaneously sending a packet to all hosts with the same network address.

Netmask

In each of the address classes previously described, the size of the two parts (network address and host address) is implied by the class. This partitioning scheme can also be expressed by a netmask associated with the IP address. A netmask is a 32-bit quantity that, when logically combined (using an AND operator) with an IP address, yields the network address. For instance, the netmasks for Class A, B, and C addresses are 255.0.0.0, 255.255.0.0, and 255.255.255.0, respectively.

For example, the address 192.168.170.237 is a Class C IP address whose network portion is the upper 24 bits. When combined (using an AND operator) with the Class C netmask, as shown here, only the network portion of the address remains:

```
11000000  10101000  10101010  11101101 (192.168.170.237)
```

combined with:

```
11111111  11111111  11111111  00000000 (255.255.255.0)
```

Equals:

```
11000000  10101000  10101010  00000000 (192.168.170.0)
```

As a shorter alternative to dotted-decimal notation, the netmask may also be expressed in terms of the number of ones from the left. This number is appended to the IP address, following a backward slash (/), as "/n." In the example, the address could be written as 192.168.170.237/24, indicating that the netmask is 24 ones followed by 8 zeros.

Subnet Addressing

By looking at the addressing structures, you can see that even with a Class C address, there are a large number of hosts per network. Such a structure is an inefficient use of addresses if each end of a routed link requires a different network number. It is unlikely that the smaller office LANs would have that many devices. You can resolve this problem by using a technique known as subnet addressing.

Subnet addressing allows us to split one IP network address into smaller multiple physical networks known as subnetworks. Some of the node numbers are used as a subnet number instead. A Class B address gives us 16 bits of node numbers translating to 64,000 nodes. Most organizations do not use 64,000 nodes, so there are free bits that can be reassigned. Subnet addressing makes use of those bits that are free, as shown below.

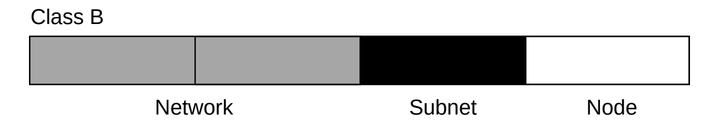


Figure C-2: Example of Subnetting a Class B Address

A Class B address can be effectively translated into multiple Class C addresses. For example, the IP address of 172.16.0.0 is assigned, but node addresses are limited to 255 maximum, allowing eight extra bits to use as a subnet address. The IP address of 172.16.97.235 would be interpreted as IP network address 172.16, subnet number 97, and node number 235. In addition to extending the number of addresses available, subnet addressing provides other benefits. Subnet addressing allows a network manager to construct an address scheme for the network by using different subnets for other geographical locations in the network or for other departments in the organization.

Although the preceding example uses the entire third octet for a subnet address, note that you are not restricted to octet boundaries in subnetting. To create more network numbers, you need only shift some bits from the host address to the network address. For instance, to partition a Class C network number (192.68.135.0) into two, you shift one bit from the host address to the network address. The new netmask (or subnet mask) is 255.255.255.128. The first subnet has network number 192.68.135.0 with hosts 192.68.135.1 to 129.68.135.126, and the second subnet has network number 192.68.135.128 with hosts 192.68.135.129 to 192.68.135.254.



Note: The number 192.68.135.127 is not assigned because it is the broadcast address of the first subnet. The number 192.68.135.128 is not assigned because it is the network address of the second subnet.

The following table lists the additional subnet mask bits in dotted-decimal notation. To use the table, write down the original class netmask and replace the 0 value octets with the dotted-decimal value of the additional subnet bits. For example, to partition your Class C network with subnet mask 255.255.255.0 into 16 subnets (4 bits), the new subnet mask becomes 255.255.255.240.

Table C-1. Netmask Notation Translation Table for One Octet

Number of Bits	Dotted-Decimal Value
1	128
2	192
3	224
4	240
5	248
6	252
7	254
8	255

The following table displays several common netmask values in both the dotted-decimal and the masklength formats.

Table C-2. Netmask Formats

Dotted-Decimal	Masklength
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30
255.255.255.254	/31
255.255.255.255	/32

Configure all hosts on a LAN segment to use the same netmask for the following reasons:

- So that hosts recognize local IP broadcast packets

  When a device broadcasts to its segment neighbors, it uses a destination address of the local network address with all ones for the host address. In order for this scheme to work, all devices on the segment must agree on which bits comprise the host address.

- So that a local router or bridge recognizes which addresses are local and which are remote

Private IP Addresses

If your local network is isolated from the Internet (for example, when using NAT), you can assign any IP addresses to the hosts without problems. However, the IANA has reserved the following three blocks of IP addresses specifically for private networks:

```
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255
```

Choose your private network number from this range. The DHCP server of the WG602 v3 Access Point is preconfigured to automatically assign private addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines explained here. For more information about address assignment, refer to RFC 1597, *Address Allocation for Private Internets*, and RFC 1466, *Guidelines for Management of IP Address Space*. The Internet Engineering Task Force (IETF) publishes RFCs on its Web site at www.ietf.org.

Single IP Address Operation Using NAT

In the past, if multiple PCs on a LAN needed to access the Internet simultaneously, you had to obtain a range of IP addresses from the ISP. This type of Internet account is more costly than a single-address account typically used by a single user with a modem, rather than a router. The WG602 v3 Access Point employs an address-sharing method called Network Address Translation (NAT). This method allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your ISP.

The router accomplishes this address sharing by translating the internal LAN IP addresses to a single address that is globally unique on the Internet. The internal LAN IP addresses can be either private addresses or registered addresses. For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

The following figure illustrates a single IP address operation.

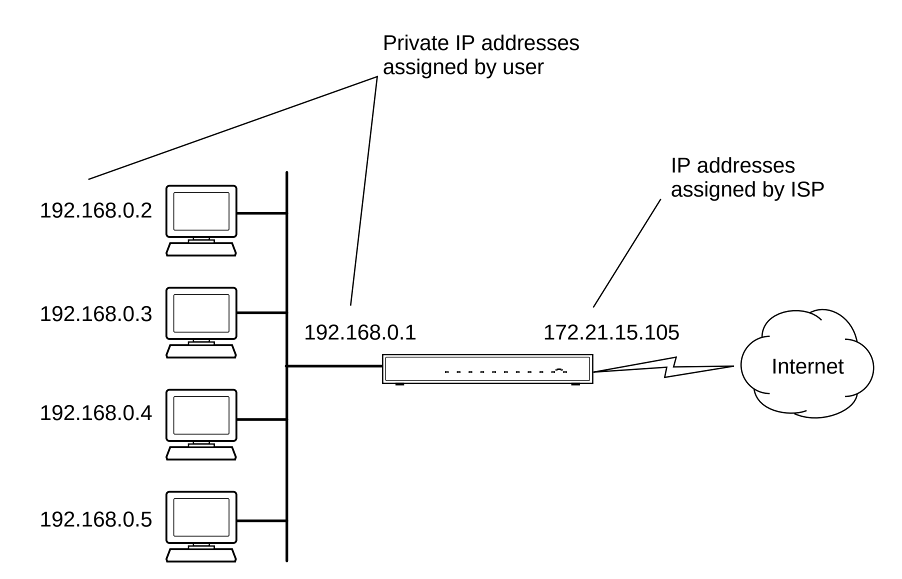


Figure C-3: Single IP Address Operation Using NAT

This scheme offers the additional benefit of firewall-like protection because the internal LAN addresses are not available to the Internet through the translated connection. All incoming inquiries are filtered out by the router. This filtering can prevent intruders from probing your system. However, using port forwarding, you can allow one PC (for example, a Web server) on your local network to be accessible to outside users.

For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

IP Configuration by DHCP

When an IP-based local area network is installed, each PC must be configured with an IP address. If the PCs need to access the Internet, they should also be configured with a gateway address and one or more DNS server addresses. As an alternative to manual configuration, there is a method by which each PC on the network can automatically obtain this configuration information. A device on the network may act as a Dynamic Host Configuration Protocol (DHCP) server. The DHCP server stores a list or pool of IP addresses, along with other information (such as gateway and DNS addresses) that it may assign to the other devices on the network. The WG602 v3 Access Point has the capacity to act as a DHCP server.

The WG602 v3 Access Point also functions as a DHCP client when connecting to the ISP. The firewall can automatically obtain an IP address, subnet mask, DNS server addresses, and a gateway address if the ISP provides this information by DHCP.

Domain Name Server

Many of the resources on the Internet can be addressed by simple descriptive names such as *www.netgear.com*. This addressing is very helpful at the application level, but the descriptive name must be translated to an IP address in order for a user to actually contact the resource. Just as a telephone directory maps names to phone numbers, or as an ARP table maps IP addresses to MAC addresses, a domain name system (DNS) server maps descriptive names of network resources to IP addresses.

When a PC accesses a resource by its descriptive name, it first contacts a DNS server to obtain the IP address of the resource. The PC sends the desired message using the IP address. Many large organizations, such as ISPs, maintain their own DNS servers and allow their customers to use the servers to look up addresses.

Routing Protocols

Two protocols routers use extensively are:

- Routing Information Protocol (RIP)
- Address Resolution Protocol (ARP)

These two protocols are introduced below.

RIP

One of the protocols used by a router to build and maintain a picture of the network is RIP. Using RIP, routers periodically update one another and check for changes to add to the routing table.

The WG602 v3 Access Point supports both the older RIP-1 and the newer RIP-2 protocols. Among other improvements, RIP-2 supports subnet and multicast protocols. RIP is not required for most home applications.

MAC Addresses and ARP

An IP address alone cannot be used to deliver data from one LAN device to another. To send data between LAN devices, you must convert the IP address of the destination device to its media access control address (MAC address). Each device on an Ethernet network has a unique MAC address, which is a 48-bit number assigned to each device by the manufacturer. The technique that associates the IP address with a MAC address is known as address resolution. Internet Protocol uses the ARP to resolve MAC addresses.

If a device sends data to another station on the network and the destination MAC address is not yet recorded, ARP is used. An ARP request is broadcast onto the network. All stations on the network receive and read the request. The destination IP address for the chosen station is included as part of the message so that only the station with this IP address responds to the ARP request. All other stations discard the request.

The station with the correct IP address responds with its own MAC address directly to the sending device. The receiving station provides the transmitting station with the required destination MAC address. The IP address data and MAC address data for each station are held in an ARP table. The next time data is sent, the address can be obtained from the address information in the table.

For more information about address assignment, refer to the IETF documents RFC 1597, *Address Allocation for Private Internets*, and RFC 1466, *Guidelines for Management of IP Address Space*.

Internet Security and Firewalls

When your LAN connects to the Internet through a router, an opportunity is created for outsiders to access or disrupt your network. A NAT router provides some protection because by the very nature of the process, the network behind the router is shielded from access by outsiders on the Internet. However, there are methods by which a determined hacker can possibly obtain information about your network or at the least can disrupt your Internet access. A greater degree of protection is provided by a firewall router.

What is a Firewall?

A firewall is a device that protects one network from another, while allowing communication between the two. A firewall incorporates the functions of the NAT router, while adding features for dealing with a hacker intrusion or attack. Several known types of intrusion or attack can be recognized when they occur. When an incident is detected, the firewall can log details of the attempt, and can optionally send email to an administrator notifying them of the incident. Using information from the log, the administrator can take action with the ISP of the hacker. In some types of intrusions, the firewall can fend off the hacker by discarding all further packets from the hacker's IP address for a period of time.

Stateful Packet Inspection

Unlike simple Internet sharing routers, a firewall uses a process called stateful packet inspection to ensure secure firewall filtering to protect your network from attacks and intrusions. Since user-level applications such as FTP and Web browsers can create complex patterns of network traffic, it is necessary for the firewall to analyze groups of network connection states. Using Stateful Packet Inspection, an incoming packet is intercepted at the network layer and then analyzed for state-related information associated with all network connections. A central cache within the firewall keeps track of the state information associated with all network connections. All traffic passing through the firewall is analyzed against the state of these connections in order to determine whether or not it will be allowed to pass through or rejected.

Denial of Service Attack

A hacker may be able to prevent your network from operating or communicating by launching a Denial of Service (DoS) attack. The method used for such an attack can be as simple as merely flooding your site with more requests than it can handle. A more sophisticated attack may attempt to exploit some weakness in the operating system used by your router or gateway. Some operating systems can be disrupted by simply sending a packet with incorrect length information.

Ethernet Cabling

Although Ethernet networks originally used thick or thin coaxial cable, most installations currently use unshielded twisted pair (UTP) cabling. The UTP cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. A normal straight-through UTP Ethernet cable follows the EIA568B standard wiring as described below in Table C-1

.

Table C-1. UTP Ethernet cable wiring, straight-through

Pin	Wire color	Signal
1	Orange/White	Transmit (Tx) +
2	Orange	Transmit (Tx) -
3	Green/White	Receive (Rx) +
4	Blue	
5	Blue/White	
6	Green	Receive (Rx) -
7	Brown/White	
8	Brown	

Category 5 Cable Quality

Category 5 distributed cable that meets ANSI/EIA/TIA-568-A building wiring standards can be a maximum of 328 feet (ft.) or 100 meters (m) in length, divided as follows:

20 ft. (6 m) between the hub and the patch panel (if used)

295 ft. (90 m) from the wiring closet to the wall outlet

10 ft. (3 m) from the wall outlet to the desktop device

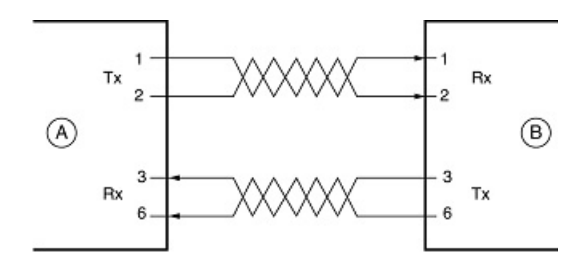
The patch panel and other connecting hardware must meet the requirements for 100 Mbps operation (Category 5). Only 0.5 inch (1.5 cm) of untwist in the wire pair is allowed at any termination point.

A twisted pair Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (10BASE-Tx) the cable must be rated as Category 5, or Cat 5, by the Electronic Industry Association (EIA). This rating will be printed on the cable jacket. A Category 5 cable will meet specified requirements regarding loss and crosstalk. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.

Inside Twisted Pair Cables

For two devices to communicate, the transmitter of each device must be connected to the receiver of the other device. The crossover function is usually implemented internally as part of the circuitry in the device. Computers and workstation adapter cards are usually media-dependent interface ports, called MDI or uplink ports. Most repeaters and switch ports are configured as media-dependent interfaces with built-in crossover ports, called MDI-X or normal ports. Auto Uplink technology automatically senses which connection, MDI or MDI-X, is needed and makes the right connection.

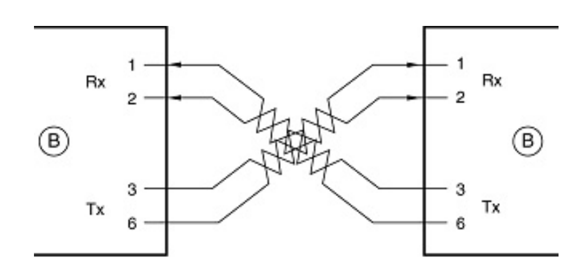
Figure C-4 illustrates straight-through twisted pair cable.



Key:
A = UPLINK OR MDI PORT (as on a PC)
B = Normal or MDI-X port (as on a hub or switch)
1, 2, 3, 6 = Pin numbers

Figure C-4: Straight-Through Twisted-Pair Cable

Figure C-5 illustrates crossover twisted pair cable.



Key:
B = Normal or MDI-X port (as on a hub or switch)
1, 2, 3, 6 = Pin numbers

Figure C-5: Crossover Twisted-Pair Cable

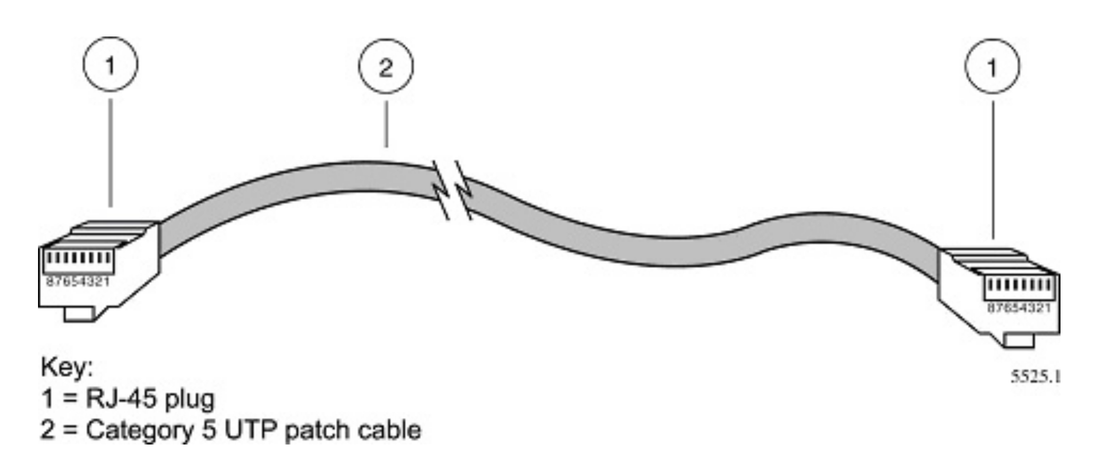


Figure C-6: Category 5 UTP Cable with Male RJ-45 Plug at Each End

Note: Flat "silver satin" telephone cable may have the same RJ-45 plug. However, using telephone cable results in excessive collisions, causing the attached port to be partitioned or disconnected from the network.

Uplink Switches, Crossover Cables, and MDI/MDIX Switching

In the wiring table above, the concept of transmit and receive are from the perspective of the PC, which is wired as Media Dependant Interface (MDI). In this wiring, the PC transmits on pins 1 and 2. At the hub, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X).

When connecting a PC to a PC, or a hub port to another hub port, the transmit pair must be exchanged with the receive pair. This exchange is done by one of two mechanisms. Most hubs provide an Uplink switch which will exchange the pairs on one port, allowing that port to be connected to another hub using a normal Ethernet cable. The second method is to use a crossover cable, which is a special cable in which the transmit and receive pairs are exchanged at one of the two cable connectors. Crossover cables are often unmarked as such, and must be identified by comparing the two connectors. Since the cable connectors are clear plastic, it is easy to place them side by side and view the order of the wire colors on each. On a straight-through cable, the color order will be the same on both connectors. On a crossover cable, the orange and blue pairs will be exchanged from one connector to the other.

The WG602 v3 Access Point incorporates Auto Uplink™ technology (also called MDI/MDIX). Each LOCAL Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a normal connection (e.g. connecting to a PC) or an uplink connection (e.g. connecting to a router, switch, or hub). That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink™ will accommodate either type of cable to make the right connection.



Appendix D
Preparing Your PCs for Network Access

This appendix describes how to prepare your PCs to connect to the Internet through the 54 Mbps Wireless Access Point WG602 v3.

For adding file and print sharing to your network, please consult the Windows help information included with the version of Windows installed on each computer on your network.

Preparing Your Computers for TCP/IP Networking

Computers access the Internet using a protocol called TCP/IP (Transmission Control Protocol/ Internet Protocol). Each computer on your network must have TCP/IP installed and selected as its networking protocol. If a Network Interface Card (NIC) is already installed in your PC, then TCP/ IP is probably already installed as well.

Most operating systems include the software components you need for networking with TCP/IP. Windows 95 or later includes the software components for establishing a TCP/IP network.

In your TCP/IP network, each PC and the wireless access point must be assigned a unique IP addresses. Each PC must also have certain other TCP/IP configuration information such as a subnet mask (netmask), a domain name server (DNS) address, and a default gateway address. In most cases, you should install TCP/IP so that the PC obtains its specific network configuration information automatically from a DHCP server during startup.

Configuring Windows 98 and Me for TCP/IP Networking

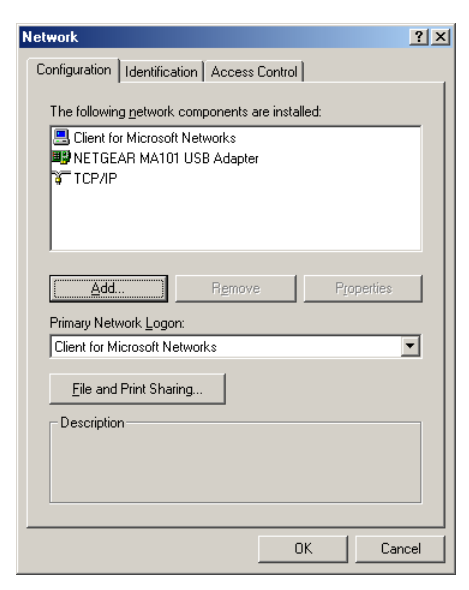
As part of the PC preparation process, you may need to install and configure TCP/IP on your PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

Installing or Verifying Windows Networking Components

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network icon.

   The Network window opens, which displays a list of installed components:



   You must have an Ethernet adapter or an WG602 v3, the TCP/IP protocol, and the Client for Microsoft Networks.



Note: It is not necessary to remove any other network components shown in the Network window in order to install the adapter, TCP/IP, or Client for Microsoft Networks.

If you need to add TCP/IP:

a. Click the Add button.
b. Select Protocol, and then click Add.
c. Select Microsoft.
d. Select TCP/IP, and then click OK.

If you need to add the Client for Microsoft Networks:

a. Click the Add button.
b. Select Client, and then click Add.
c. Select Microsoft.
d. Select Client for Microsoft Networks, and then click OK.

If you need to add File and Print Sharing for Microsoft Networks:

a. Click the Add button.
b. Select Client, and then click Add.
c. Select Microsoft.
d. Select File and Print Sharing for Microsoft Networks, and then click OK.

3. Restart your PC for the changes to take effect.

Enabling DHCP to Automatically Configure TCP/IP Settings

After the TCP/IP protocol components are installed, each PC must be assigned specific information about itself and resources that are available on its network. The simplest way to configure this information is to allow the PC to obtain the information from a DHCP server in the network.

You will find there are many similarities in the procedures for different Windows systems when using DHCP to configure TCP/IP.

The following steps will walk you through the configuration process for each of these versions of Windows.

DHCP Configuration of TCP/IP in Windows 98 and Me



In Windows 98 and Me systems, locate your **Network Neighborhood** icon.

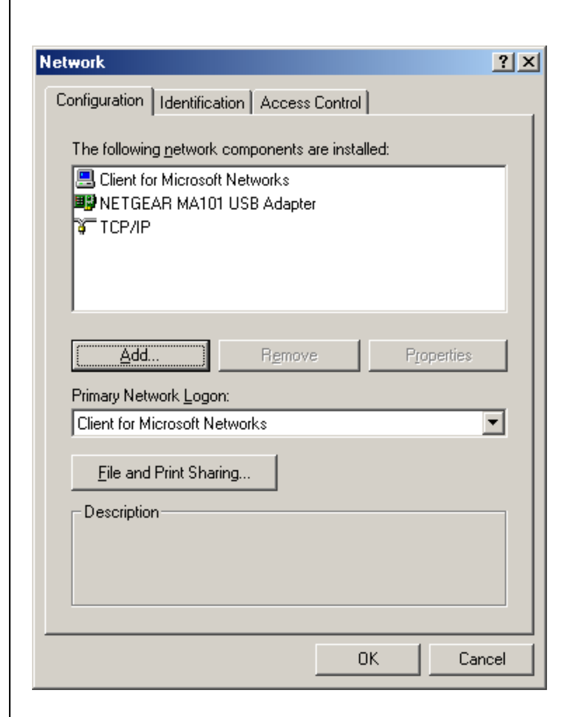
- If the Network Neighborhood icon is on the Windows desktop, position your mouse pointer over it and right-click your mouse button.
- If the icon is not on the desktop,
  - Click **Start** on the task bar located at the bottom left of the window.
  - Choose **Settings**, and then **Control Panel**.
  - Locate the **Network Neighborhood** icon and click it. This will open the Network panel as shown below.

2

Verify the following settings as shown:

- Client for Microsoft Network exists
- Ethernet adapter is present
- TCP/IP is present
- **Primary Network Logon** is set to Windows logon

Click the **Properties** button. The following TCP/IP Properties window will display.





By default, the **IP Address** tab is open on this window.

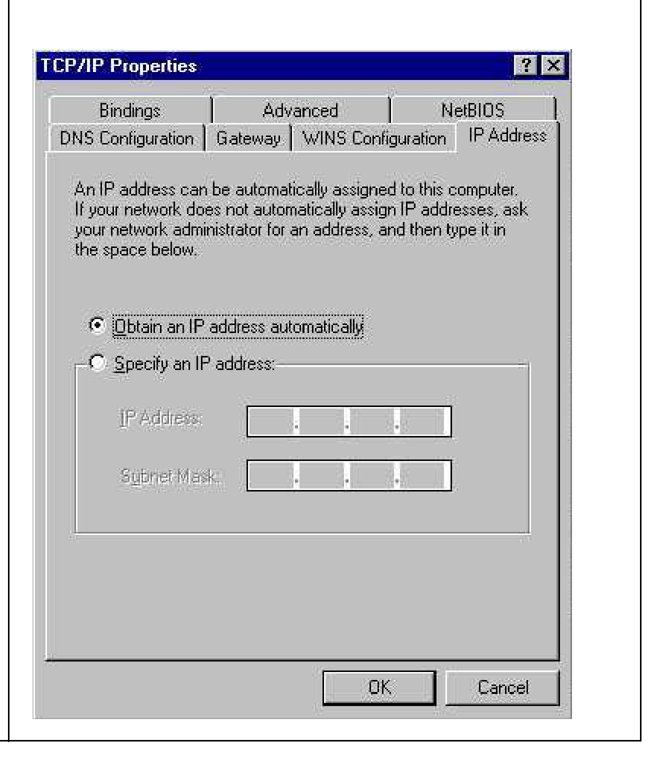
- Verify the following:

  Obtain an IP address automatically is selected. If not selected, click in the radio button to the left of it to select it. This setting is required to enable the DHCP server to automatically assign an IP address.

- Click **OK** to continue.

Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.



Selecting the Windows Internet Access Method

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Internet Options icon.
3. Select "I want to set up my Internet connection manually" or "I want to connect through a Local Area Network" and click Next.
4. Select "I want to connect through a Local Area Network" and click Next.
5. Clear all check boxes in the LAN Internet Configuration screen and click Next.
6. Proceed to the end of the Wizard.

Verifying TCP/IP Properties for Windows 98 or Me

After your PC is configured and has rebooted, you can check the TCP/IP configuration using the utility *winipcfg.exe*:

1. On the Windows taskbar, click the Start button, and then click Run.

2. Type **`winipcfg`**, and then click OK.

   The IP Configuration window opens, which lists (among other things), your IP address, subnet mask, and default gateway.

3. From the drop-down box, select your Ethernet adapter.

   The window is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends for connecting through a router or gateway:

   - The IP address is between 192.168.0.2 and 192.168.0.254
   - The subnet mask is 255.255.255.0
   - The default gateway is 192.168.0.1

Configuring Windows 2000 or XP for TCP/IP Networking

As part of the PC preparation process, you may need to install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

Installing or Verifying Windows Networking Components

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network and Dialup Connections icon.
3. If an Ethernet adapter is present in your PC, you should see an entry for Local Area Connection. Double-click that entry.
4. Select Properties.
5. Verify that 'Client for Microsoft Networks' and 'Internet Protocol (TCP/IP)' are present. If not, select Install and add them.
6. Select 'Internet Protocol (TCP/IP)', click Properties, and verify that "Obtain an IP address automatically is selected.
7. Click OK and close all Network and Dialup Connections windows.
8. Then, restart your PC.

DHCP Configuration of TCP/IP in Windows XP

You will find there are many similarities in the procedures for different Windows systems when using DHCP to configure TCP/IP.

The following steps will walk you through the configuration process for each of these versions of Windows.



In Windows XP and 2000 systems, locate your **Network Neighborhood** icon.

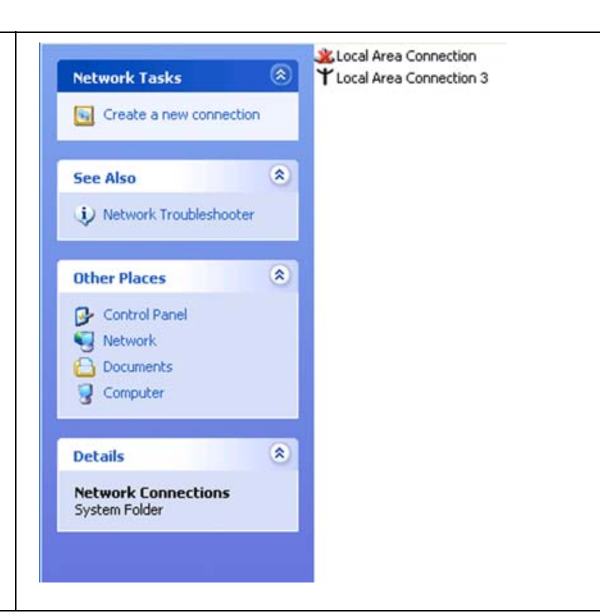
- Select **Control Panel** from the Windows XP Start Menu.
- Select the **Network Connections** icon on the Control Panel. This will take you to the next step.



Now the Network Connection window displays.

The Connections List shows all the network connections set up on the PC, located to the right of the window.

- Right-click the **Connection with the wireless** icon and choose **Status**.

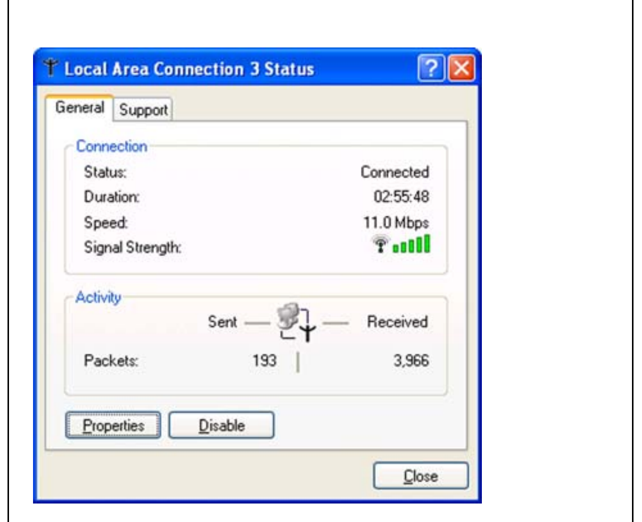


3

Now you should be at the Local Area Network Connection Status window. This box displays the connection status, duration, speed, and activity statistics.

Administrator logon access rights are needed to use this window.

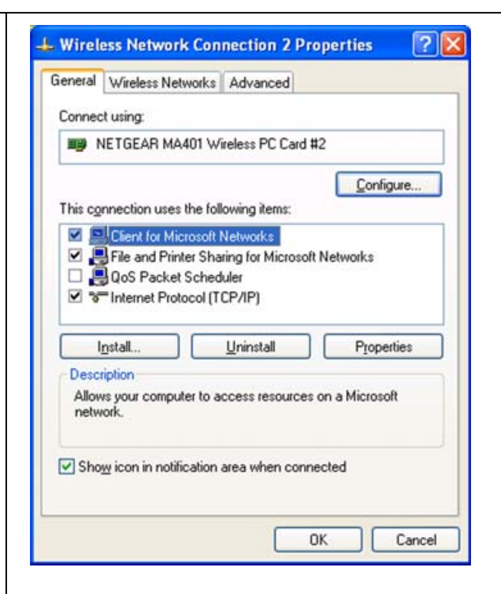
- Click the **Properties button** to view details about the connection.





The TCP/IP details are presented on the Support tab page.

- Select **Internet Protocol,** and click **Properties** to view the configuration information**.**



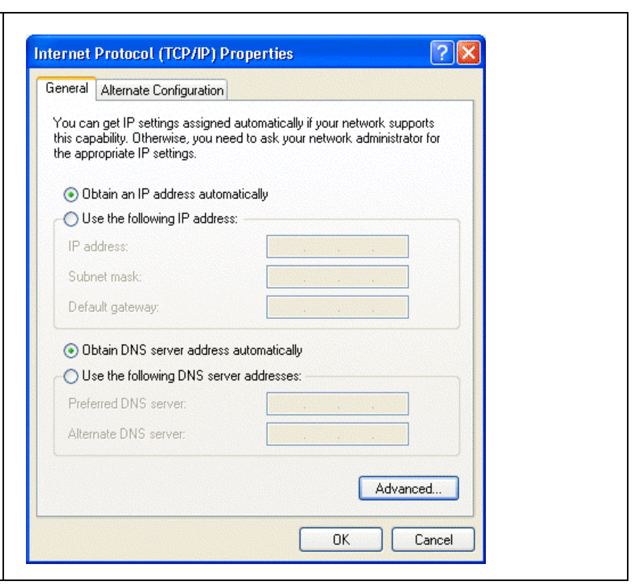


Verify that **Obtain an IP address automatically** radio button is selected and that the **Obtain DNS server address automatically** radio button is selected.

Click the **OK** button.

This completes the DHCP configuration in Windows XP.

Repeat these steps for each PC with this version of Windows on your network.



DHCP Configuration of TCP/IP in Windows 2000

After you install a network card, TCP/IP for Windows 2000 is configured and set to DHCP without your having to configure it. However, if there are problems, follow the steps below to configure TCP/IP with DHCP for Windows 2000.



Click **My Network Places** icon on the Windows desktop. This will bring up a window called Network and Dial-up Connections.

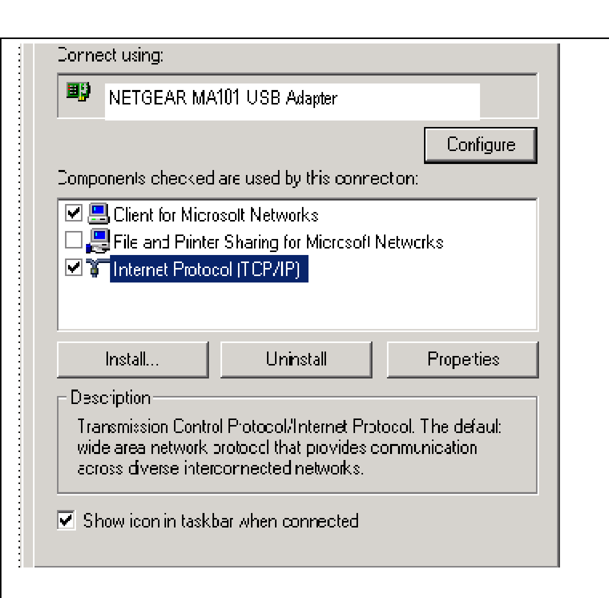
• Right click **Local Area Connection** and select **Properties**.



The **Local Area Connection Properties** dialog box appears. Verify that you have the correct Ethernet card selected in the **Connect using:** box and that the following two items are displayed and selected in the box of "Components checked are used by this connection:"

- Client for Microsoft Networks and
- Internet Protocol (TCP/IP)

Click **OK**.



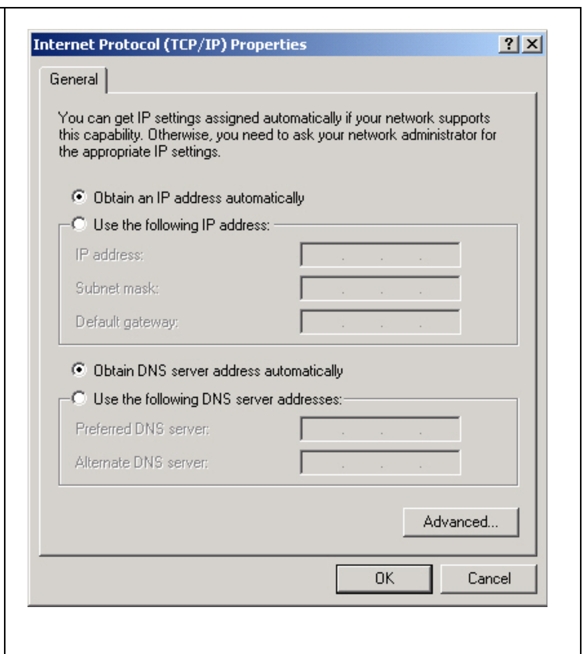
3

With Internet Protocol (TCP/IP) selected, click **Properties** to open the Internet Protocol (TCP/IP) Properties dialogue box. Verify that

- **Obtain an IP address automatically** is selected.
- **Obtain DNS server address automatically** is selected.

Click **OK** to return to Local Area Connection Properties. Click **OK** again to complete the configuration process.

Restart the PC. Repeat these steps for each PC with this version of Windows on your network.



Verifying TCP/IP Properties for Windows XP or 2000

To check your PC's TCP/IP configuration:

1. On the Windows taskbar, click the Start button, and then click Run.

   The Run window opens.

2. Type **`cmd`** and then click OK.

   A command window opens

3. Type **`ipconfig /all`**.

   Your IP Configuration information will be listed, and should match the values below if you are using the default TCP/IP settings that NETGEAR recommends for connecting through a router or gateway:

   - The IP address is between 192.168.0.2 and 192.168.0.254
   - The subnet mask is 255.255.255.0
   - The default gateway is 192.168.0.1

4. Type **`exit`**.



Glossary

Use the list below to find definitions for technical terms used in this manual.

Numeric

802.1x
802.1x defines port-based, network access control used to provide authenticated network access and automated data encryption key management.
The IEEE 802.1x draft standard offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1x uses a protocol called EAP (Extensible Authentication Protocol) and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication. For details on EAP specifically, refer to IETF's RFC 2284.

802.11a
IEEE specification for wireless networking at 54 Mbps operating in unlicensed radio bands over 5GHz.

802.11b
IEEE specification for wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5GHz.

802.11g
An IEEE specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5GHz. 802.11g is backwards compatible with 802.11b.

10BASE-T
The IEEE specification for 10 Mbps Ethernet over Category 3, 4, or 5 twisted-pair cable.

100BASE-TX
The IEEE specification for 100 Mbps Fast Ethernet over Category 5 twisted-pair cable.
gain access.

A

Access Control List

An ACL is a database that an Operating System uses to track each user’s access rights to system objects (such as file directories and/or files).

ACL

See “Access Control List”

Ad-hoc Mode

An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an access point (AP). Ad-hoc mode is also referred to as peer-to-peer mode or an Independent Basic Service Set (IBSS). Ad-hoc mode is useful for establishing a network where wireless infrastructure does not exist or where services are not required.

ADSL

Short for asymmetric digital subscriber line, a technology that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).
ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.



B

Bandwidth

The information capacity, measured in bits per second, that a channel could transmit. Bandwidth examples include 10 Mbps for Ethernet, 100 Mbps for Fast Ethernet, and 1000 Mbps (I Gbps) for Gigabit Ethernet.

Baud

The signaling rate of a line, that is, the number of transitions (voltage or frequency changes) made per second. Also known as line speed.

Broadcast

A packet sent to all devices on a network.

C

Class of Service

A term to describe treating different types of traffic with different levels of service priority. Higher priority traffic gets faster treatment during times of switch congestion

D

DHCP

See "Dynamic Host Configuration Protocol."

DNS

Short for Domain Name System (or Service), an Internet service that translates domain names into IP addresses.
Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Domain Name

A descriptive name for an address or group of addresses on the Internet. Domain names are of the form of a registered entity name plus one of a number of predefined top level suffixes such as .com, .edu, .uk, etc. For example, in the address mail.NETGEAR.com, mail is a server name and NETGEAR.com is the domain.

DoS

A hacker attack designed to prevent your computer or network from operating or communicating.

DSL

Short for digital subscriber line, but is commonly used in reference to the asymmetric version of this technology (ADSL) that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).
ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

DSLAM

DSL Access Multiplexor. The piece of equipment at the telephone company central office that provides the ADSL signal.

Dynamic Host Configuration Protocol.

DHCP is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software tracks IP addresses rather than requiring an administrator to manage the task. A new computer can be added to a network without the hassle of manually assigning it a unique IP address.

E

EAP

Extensible Authentication Protocol is a general protocol for authentication that supports multiple authentication methods.

EAP, an extension to PPP, supports such authentication methods as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards. In wireless communications using EAP, a user requests connection to a WLAN through an AP, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the AP for proof of identity, which the AP gets from the user and then sends back to the server to complete the authentication. EAP is defined by RFC 2284.

ESSID

The Extended Service Set Identification (ESSID) is a thirty-two character (maximum) alphanumeric key identifying the wireless local area network.

Ethernet

A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks transmit packets at a rate of 10 Mbps.



G

Gateway

A local device, usually a router, that connects hosts on a local network to other networks.

I

ICMP

See “Internet Control Message Protocol”

IEEE

Institute of Electrical and Electronics Engineers. This American organization was founded in 1963 and sets standards for computers and communications.

IETF

Internet Engineering Task Force. An organization responsible for providing engineering solutions for TCP/IP networks. In the network management area, this group is responsible for the development of the SNMP protocol.

IKE

Internet Key Exchange. An automated method for exchanging and managing encryption keys between two VPN devices.

Infrastructure Mode

An 802.11 networking framework in which devices communicate with each other by first going through an Access Point (AP). In infrastructure mode, wireless devices can communicate with each other or can communicate with a wired network. When one AP is connected to wired network and a set of wireless stations it is referred to as a Basic Service Set (BSS). An Extended Service Set (ESS) is a set of two or more BSSs that form a single subnetwork. Most corporate wireless LANs operate in infrastructure mode because they require access to the wired LAN in order to use services such as file servers or printers.

Internet Control Message Protocol

ICMP is an extension to the Internet Protocol (IP) that supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.

Internet Protocol

The method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it among all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

Because a message is divided into a number of packets, each packet can, if necessary, be sent by a different route across the Internet. Packets can arrive in a different order than they were sent. The Internet Protocol just delivers them. It's up to another protocol, the Transmission Control Protocol (TCP) to put them back in the right order. IP is a connectionless protocol, which means that there is no continuing connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. (The reason the packets do get put in the right order is because of TCP, the connection-oriented protocol that keeps track of the packet sequence in a message.) In the Open Systems Interconnection (OSI) communication model, IP is in Layer 3, the

Networking Layer. The most widely used version of IP today is IP version 4 (IPv4). However, IP version 6 (IPv6) is also beginning to be supported. IPv6 provides for much longer addresses and therefore for the possibility of many more Internet users. IPv6 includes the capabilities of IPv4 and any server that can support IPv6 packets can also support IPv4 packets.

IP

See "Internet Protocol"

IP Address

A four-byte number uniquely defining each host on the Internet, usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57). Ranges of addresses are assigned by Internic, an organization formed for this purpose.

ISP

Internet service provider.

L

LAN

See "Local Area Network"

Local Area Network

A communications network serving users within a limited area, such as one floor of a building. A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers and is limited to a distance of 1,500 feet. LANs can be connected together, but if modems and telephones connect two or more LANs, the larger network constitutes what is called a WAN or Wide Area Network.

M

MAC

(1) Medium Access Control. In LANs, the sublayer of the data link control layer that supports medium-dependent functions and uses the services of the physical layer to provide services to the logical link control (LLC) sublayer. The MAC sublayer includes the method of determining when a device has access to the transmission medium. (2) Message Authentication Code. In computer security, a value that is a part of a message or accompanies a message and is used to determine that the contents, origin, author, or other attributes of all or part of the message are as they appear to be. (*IBM Glossary of Computing Terms*)

MAC address
The Media Access Control address is a unique 48-bit hardware address assigned to every network interface card. Usually written in the form 01:23:45:67:89:ab.

Maximum Receive Unit
The size in bytes of the largest packet that can be sent or received.

Maximum Transmit Unit
The size in bytes of the largest packet that can be sent or received.

Mbps
Megabits per second.

MDI/MDIX
In cable wiring, the concept of transmit and receive are from the perspective of the PC, which is wired as a Media Dependant Interface (MDI). In MDI wiring, a PC transmits on pins 1 and 2. At the hub, switch, router, or access point, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X).

MTU
The size in bytes of the largest packet that can be sent or received.

N

NAT
See "Network Address Translation"

NetBIOS
Network Basic Input Output System. An application programming interface (API) for sharing services and information on local-area networks (LANs). Provides for communication between stations of a network where each station is given a name. These names are alphanumeric names, 16 characters in length.

netmask
Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router. A number that explains which part of an IP address comprises the network address and which part is the host address on that network. It can be expressed in dotted-decimal notation or as a number appended to the IP address. For example, a 28-bit mask starting from the MSB can be shown as 255.255.255.192 or as /28 appended to the IP address.

Network Address Translation

Sometimes referred to as Transparent Proxying, IP Address Overloading, or IP Masquerading. Involves use of a device called a Network Address Translator, which assigns a contrived, or logical, IP address and port number to each node on an organization's internal network and passes packets using these assigned addresses.

NIC

Network Interface Card. An adapter in a computer which provides connectivity to a network.

P

packet

A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.

Point-to-Point Protocol

PPP. A protocol allowing a computer using TCP/IP to connect directly to the Internet.

PPP

A protocol allowing a computer using TCP/IP to connect directly to the Internet.

PPPoA

PPPoA. PPP over ATM is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPPoE

PPPoE. PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPP over ATM

PPPoA. PPP over ATM is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPP over Ethernet

PPPoE. PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPTP

Point-to-Point Tunneling Protocol. A method for establishing a virtual private network (VPN) by embedding Microsoft's network protocol into Internet packets.

Protocol
A set of rules for communication between devices on a network.

PSTN
Public Switched Telephone Network.

Q

QoS
See "Quality of Service"

Quality of Service
QoS is a networking term that specifies a guaranteed level of throughput. Throughput is the amount of data transferred from one device to another or processed in a specified amount of time - typically, throughputs are measured in bytes per second (Bps).

R

RADIUS
Short for Remote Authentication Dial-In User Service, RADIUS is an authentication system. Using RADIUS, you must enter your user name and password before gaining access to a network. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access. Though not an official standard, the RADIUS specification is maintained by a working group of the IETF.

RFC
Request For Comment. Refers to documents published by the Internet Engineering Task Force (IETF) proposing standard protocols and procedures for the Internet. RFCs can be found at *www.ietf.org*.

router
A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

S

SSID
A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must

be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name. *See also* Wireless Network Name and ESSID.

Segment
A section of a LAN that is connected to the rest of the network using a switch, bridge, or repeater.

Subnet Mask
Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.

T

TCP/IP
The main internetworking protocols used in the Internet. The Internet Protocol (IP) used in conjunction with the Transfer Control Protocol (TCP) form TCP/IP.



Universal Plug and Play
UPnP. A networking architecture that provides compatibility among networking technology. UPnP compliant routers provide broadband users at home and small businesses with a seamless way to participate in online games, videoconferencing and other peer-to-peer services.

UTP
Unshielded twisted pair is the cable used by 10BASE-T and 100BASE-Tx Ethernet networks.



WAN
See "Wide Area Network"

Web
Also known as World-Wide Web (WWW) or W3. An Internet client-server system to distribute information, based upon the hypertext transfer protocol (HTTP).

WEB Proxy Server

A Web proxy server is a specialized HTTP server that allows clients access to the Internet from behind a firewall. The proxy server listens for requests from clients within the firewall and forwards these requests to remote Internet servers outside the firewall. The proxy server reads responses from the external servers and then sends them to internal client clients.

WEP

Wired Equivalent Privacy is a data encryption protocol for 802.11b wireless networks.
All wireless nodes and access points on the network are configured with a 64-bit or 128-bit Shared Key for data encryption.

Wide Area Network

A WAN is a computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).

Wi-Fi

A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.

Windows Internet Naming Service

WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.
If a remote network contains a WINS server, your Windows PCs can gather information from that WINS server about its local hosts. This allows your PCs to browse that remote network using the Windows Network Neighborhood feature.

WINS

WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.

Wireless Network Name (SSID)

Wireless Network Name (SSID) is the name assigned to a wireless network. This is the same as the SSID or ESSID configuration parameter.

WPA

Wi-Fi Protected Access (WPA) is a specification of standards-based, interoperable security enhancements that increase the level of data protection and access control for existing and future wireless LAN systems.

Index

Numerics

A

B

C

D

E

F

G

I

L

M

N